

SYSTEM AND METHOD OF RENDERING DATA-SETS FOR DIFFERENTIATING A PLURALITY OF POTENTIAL THREAT ACTORS

ABSTRACT

5 Disclosed is a system and method of rendering data-sets for differentiation of insider threat actors and external threat actors. The method integrates a user action tracking (UAT) module into global keystroke and mouse hooks of an operating system (OS) through an integration module. The method then detects user action events through a first detection module to generate a first detection data. Then the method captures a foreground application process identifier (ID) on detection of the user action events through the UAT module to generate a software signal. 10 The method then records the user action events and the application process ID into an operating system (OS) logging facility through the UAT module. Further, the method detects hardware inputs about keyboard and mouse through a second detection module to generate a second detection data. The second detection module is configured within a computing device. The method then records the second detected data and an operating system (OS) instrumentation service through the computing device to generate a hardware signal. Then the method determines a physical interaction of the user based on the software signal and the hardware signal through a central module. The central module then detects the potential threat actors on determining an absence of the software signal and the hardware signal. 15 20

The most illustrative drawing: FIG. 2