

CLAIMS:

1. A computer-implemented method comprising:

integrating, by one or more processors (202), a user action tracking (UAT) module (216)
 5 into a plurality of global keystroke and mouse hooks of an operating system (OS) through
 an integration module (212);

detecting, by one or more processors (202), a plurality of user action events initiated by a
 user through a first detection module (214) to generate a first detection data, wherein the
 plurality of user action events comprises a mouse clicking event, a mouse movement event,
 10 and a key pressing event;

capturing, by one or more processors (202), a foreground application process identifier (ID)
 on detection of the user action events through the user action tracking (UAT) module (216)
 to generate a software signal based on the first detection data;

recording, by one or more processors (202), the plurality of user action events and the
 15 application process identifier (ID) into an operating system (OS) logging facility through
 the user action tracking (UAT) module (216);

detecting, by one or more processors (202), a plurality of hardware inputs pertaining to a
 keyboard and a mouse through a second detection module (218) to generate a second
 detection data, wherein the second detection module is configured within a computing
 20 device (108);

recording, by one or more processors (202), the second detected data and an operating
 system (OS) instrumentation service through the computing device (108) to generate a
 hardware signal; and

determining, by one or more processors (202), a physical interaction of the user based on
 25 the software signal received from the user action tracking (UAT) module (216) and the
 hardware signal received from the computing device (108) through a central module (220),
 wherein the central module (220) detects a plurality of potential threat actors on
 determining an absence of at least one of the software signal, the hardware signal, and/or a
 combination thereof, wherein the potential threat actors comprise a network security threat

actor, a communication threat actor, a software threat actor, a human threat actor, and a physical security threat actor.

2. The method according to claim 1, wherein the plurality of hardware inputs comprises a mouse input, a keyboard input, a trackpad input, a touch input, a video input, and/or a combination thereof, further the plurality of hardware inputs lead to create the process or to terminate the process to initiate a plurality of active foreground transitions, wherein the computing device records the plurality of active foreground transitions.
3. The method according to claim 1, wherein the foreground application process identifier (ID) is a numeric or a test-string value to identify an active foreground process (AFP), wherein the recorded plurality of user action events and the application process identifier (ID) are transferable to a plurality of centralized log collectors and a plurality of detection units.
4. The method according to claim 1, wherein the hardware signals generated by the computing device (108) utilizes an out-of-band channel to transmit the second detected data to a centralized management service unit for recording, further the centralized management service unit transmits the recorded second detected data to the detection units.
5. A system (102) comprising:
 - a memory (206) to store machine-readable instructions pertaining to rendering data-sets for differentiating a plurality of potential threat actors; and
 - a processor (202) coupled to the memory and operable to execute the machine-readable instructions stored in the memory, wherein the processor (202) comprises:
 - an integration module (212) to integrate a user action tracking (UAT) module (216) into a plurality of global keystroke and mouse hooks of an operating system (OS);
 - a first detection module (214) to detect a plurality of user action events initiated by a user to generate a first detection data, wherein the plurality of user action events comprises a mouse clicking event, a mouse movement event, and a key pressing event;
 - the user action tracking (UAT) module (216) captures a foreground application process identifier (ID) on detection of the user action events to generate a software signal based on the first detection data;

the user action tracking (UAT) module (216) records the plurality of user action events and the application process identifier (ID) into an operating system (OS) logging facility;

a second detection module (218) to detect a plurality of hardware inputs pertaining to a keyboard and a mouse to generate a second detection data, wherein the second detection module (218) is configured within a computing device (108);

the computing device (108) records the second detected data and an operating system (OS) instrumentation service to generate a hardware signal; and

a central module (220) to determine a physical interaction of the user based on the software signal received from the user action tracking (UAT) module (216) and the hardware signal received from the computing device (108), wherein the central module (220) detects a plurality of potential threat actors on determining an absence of at least one of the software signal, the hardware signal, and/or a combination thereof, wherein the potential threat actors comprise a network security threat actor, a communication threat actor, a software threat actor, a human threat actor, and a physical security threat actor.

6. The system according to claim 5, wherein the plurality of hardware inputs comprises a mouse input, a keyboard input, a trackpad input, a touch input, a video input, and/or a combination thereof, further the plurality of hardware inputs lead to create the process or to terminate the process to initiate a plurality of active foreground transitions, wherein the computing device records the plurality of active foreground transitions.

7. The system according to claim 5, wherein the foreground application process identifier (ID) is a numeric or a test-string value to identify an active foreground process (AFP), wherein the recorded plurality of user action events and the application process identifier (ID) are transferable to a plurality of centralized log collectors and a plurality of detection units.

8. The system according to claim 5, wherein the hardware signals generated by the computing device utilizes (108) an out-of-band channel to transmit the second detected data to a centralized management service unit for recording, further the centralized management service unit transmits the recorded second detected data to the detection units.