I claim :

1. An apparatus for Internet of Things (IoT) security, comprising:

an IoT hub including one or more devices, the devices including at least one memory adapted to store run-time data for the devices, and at least one processor that is adapted to execute processor-executable code that, in response to execution, enables the IoT hub to perform actions, including:

storing a set of security rules that are associated with an expected condition of at least one IoT device, the set of security rules being based on operating information received from each of a plurality of IoT devices;

receiving IoT data associated with the at least one IoT device, wherein the IoT data is aggregated data that includes at least two different types of data;

making a determination, for each IoT device of the at least one IoT device, based on the IoT data, as to whether the set of security rules has been violated for the IoT device based on operating information received from each of the plurality of IoT devices, such that the determination is based on a combination of at least two different types of data from at least two of the plurality of IoT devices considered together; and

selectively sending an alert based on the determination.

2. The apparatus of claim 1, the actions further including:

receiving a configuration request; and

adjusting the set of security rules based on the configuration request.

3. The apparatus of claim 1, wherein the IoT data is received from a data collection agent deployed on the at least one IoT device.

4. The apparatus of claim 1, wherein the at least one IoT device includes a plurality of IoT devices, and wherein the IoT data is received from data collection agents deployed on the plurality of IoT devices.

5. The apparatus of claim 1, wherein the set of security rules include at least one of a whitelist of processes or a blacklist of processes.

6. The apparatus of claim 1, wherein the IoT data includes a state of a tampering switch on the at least one IoT device.

7. The apparatus of claim 1, wherein the IoT data is aggregated from multiple IoT devices including the at least one IoT device.

8. The apparatus of claim 1, wherein the aggregated data of the IoT data includes environmental data and internal state data.

9. The apparatus of claim 8, wherein the environmental data includes at least one of temperature, humidity, sensed location, or geolocation.

10. The apparatus of claim 8, wherein the internal data includes at least one of operating system version, a current state of active processes, open ports, or information associated with devices connected to the at least one IoT device.

11. The apparatus of claim 1, wherein the set of security rules are such that violation of the set of security rules indicates at least a possibility of an attack, wherein the attack is at least one of a physical attack or a cyber attack on the at least one IoT device.

12. The apparatus of claim 11, selectively sending the alert based on the determination further includes selectively sending information about the attack with the alert.

13. A method for Internet of Things (IoT) security, comprising:

generating a configurable IoT device model based on operating information received from each of a plurality of IoT devices;

receiving aggregated IoT device data from at least one IoT device, wherein the aggregated data IoT device data includes at least two different types of data from the plurality of IoT devices;

employing at least one processor to compare the aggregated IoT device data with the configurable IoT device model such that the comparison is adjudicated based on a combination of at least two different types of data from at least two of the plurality of IoT devices considered together; and

selectively sending an alert based on the comparison.

14. The method of claim 13, wherein the at least one IoT device includes a plurality of IoT devices, and wherein the aggregated IoT device data is received from data collection agents deployed on the plurality of IoT devices.

15. The method of claim 13, wherein the aggregated data IoT device data includes environmental data and internal state data.

16. The method of claim 13, further comprising:

receiving a configuration request; and

adjusting the configurable IoT device model based on the configuration request.

17. A method for Internet of Things (IoT) security, comprising:

employing at least one processor to generate a configuration request, wherein the configuration request is a request to change a set of security rules to an adjusted set of security rules, wherein the adjusted set of security rules is associated with an expected condition of at least one IoT device, wherein the adjusted set of security rules is based upon an assessment of IoT data associated with each of a plurality of IoT devices, and wherein the IoT data is aggregated data that includes at least two different types of data from the plurality of IoT devices such that the applying the adjusted set of security rules is

based on a combination of at least two different types of data from at least two of the plurality of IoT devices considered together;

sending the configuration request to an IoT hub; and

receiving an alert from the IoT hub upon the IoT hub making a determination that the adjusted set of security rules has been violated.

18. The method of claim 17, wherein the adjusted set of security rules are based upon an assessment of IoT data associated with the at least one IoT device such that the at least one IoT device is a plurality of IoT devices.

19. The method of claim 17, wherein the aggregated data of the IoT data includes environmental data and internal data.

20. The method of claim 19, wherein the environmental data includes at least one of temperature, humidity, sensed location, or geolocation, and wherein the internal data includes at least one of operating system version, a current state of active processes, open ports, or information associated with devices connected to the at least one IoT device.