CLAIMS

1. A computer-implemented method for a security model, comprising:
generating a Bloch sphere based on a system information and event management (SIEM) of a security domain and a structured threat information expression trusted automated exchange of indicator information (STIX-TAXII);
generating a quantum state probabilities matrix based on the Bloch sphere;
training a security threat model to perform security threat classifications based on the quantum state probabilities matrix; and
performing a machine learning classification of the security domain based on the quantum state probabilities matrix, wherein the quantum state probabilities matrix comprises a plurality of probabilities representing:
a likelihood that a malicious actor moves between all potential combinations of categories of attack; and
a likelihood that the malicious actor uses a specific attack method of all of the categories of attack based on a previous category of attack.

2. The method of claim 1, further comprising determining that a malicious actor performs a specific category of attack based on a previous category of attack and the quantum state probabilities matrix.

3. The method of claim 2, further comprising determining that the malicious actor performs a specific attack method of the specific category of attack based on the specific category of attack and the quantum state probabilities matrix.

4. The method of claim 1, further comprising determining that a plurality of malicious actors is performing a game theory attack.

5. The method of claim 4, wherein determining that the malicious actors are performing the game theory attack comprises:
generating a plurality of quantum state probabilities matrices for movements between a plurality of pairs of categories of attack; and
determining that a plurality of probabilities overlap between two or more of the plurality of quantum state probabilities matrices.

6. The method of claim 1, wherein the likelihood that the malicious actor moves between a combination of the categories of attack comprises a plurality of likelihoods that the malicious actor performs a plurality of specific attack methods of a specific category of attack.

7. The method of claim 1, wherein the Bloch sphere comprises:
an origin; and
three axes representing three-dimensional space, wherein one of the three axes represent a time that an attack

method is performed.

8. A computer program product comprising program instructions stored on a computer readable storage medium, the program instructions executable by a processor to cause the processor to perform a method comprising:

generating a Bloch sphere based on a system information and event management (SIEM) of a security domain and a structured threat information expression trusted automated exchange of indicator information (STIX-TAXII);

generating a quantum state probabilities matrix based on the Bloch sphere;

training a security threat model to perform security threat classifications based on the quantum state probabilities matrix; and

performing a machine learning classification of the security domain based on the quantum state probabilities matrix, wherein the quantum state probabilities matrix comprises a plurality of probabilities representing:

a likelihood that a malicious actor moves between all potential combinations of categories of attack; and

a likelihood that the malicious actor uses a specific attack method of all of the categories of attack based on a previous category of attack.

9. The computer program product of claim 8, further comprising determining that a malicious actor performs a specific category of attack based on a previous category of attack and the quantum state probabilities matrix.

10. The computer program product of claim 9, further comprising determining that the malicious actor performs a specific attack method of the specific category of attack based on the specific category of attack and the quantum state probabilities matrix.

11. The computer program product of claim 8, further comprising determining that a plurality of malicious actors is performing a game theory attack.

12. The computer program product of claim 11, wherein determining that the malicious actors are performing the game theory attack comprises:

generating a plurality of quantum state probabilities matrices for movements between a plurality of pairs of categories of attack; and

determining that a plurality of probabilities overlap between two or more of the plurality of quantum state probabilities matrices.

13. The computer program product of claim 8, wherein the likelihood that the malicious actor moves between a combination of the categories of attack comprises a plurality of likelihoods that the malicious actor performs a plurality of specific attack methods of a specific category of attack.

14. The computer program product of claim 8, wherein the Bloch sphere comprises:

an origin; and

three axes representing three-dimensional space, wherein one of the three axes represent a time that an attack method is performed.

15. A system comprising:

a computer processing circuit; and

a computer-readable storage medium storing instructions, which, when executed by the computer processing circuit, are configured to cause the computer processing circuit to perform a method comprising:

generating a Bloch sphere based on a system information and event management (SIEM) of a security domain and a structured threat information expression trusted automated exchange of indicator information (STIX-TAXII);

generating a quantum state probabilities matrix based on the Bloch sphere;

training a security threat model to perform security threat classifications based on the quantum state probabilities matrix; and

performing a machine learning classification of the security domain based on the quantum state probabilities matrix, wherein the quantum state probabilities matrix comprises a plurality of probabilities representing:

a likelihood that a malicious actor moves between all potential combinations of categories of attack; and

a likelihood that the malicious actor uses a specific attack method of all of the categories of attack based on a previous category of attack.

16. The system of claim 15, further comprising:

determining that a malicious actor performs a specific category of attack based on a previous category of attack and the quantum state probabilities matrix; and

determining that the malicious actor performs a specific attack method of the specific category of attack based on the specific category of attack and the quantum state probabilities matrix.

17. The system of claim 15, further comprising determining that a plurality of malicious actors is performing a game theory attack, wherein determining that the malicious actors are performing the game theory attack comprises:

generating a plurality of quantum state probabilities matrices for movements between a plurality of pairs of categories of attack; and

determining that a plurality of probabilities overlap between two or more of the plurality of quantum state probabilities matrices.

18. The system of claim 15, wherein the likelihood that the malicious actor moves between a combination of the categories of attack comprises a plurality of likelihoods that the malicious actor performs a plurality of specific attack methods of a specific category of attack.

19. The system of claim 15, wherein the Bloch sphere comprises:

an origin; and

three axes representing three-dimensional space, wherein one of the three axes represent a time that an attack method is performed.

20. A computer-implemented method for a security model, comprising:

generating a Bloch sphere based on a system information and event management (SIEM) of a security domain and a structured threat information expression trusted automated exchange of indicator information (STIX-TAXII);

generating a quantum state probabilities matrix based on the Bloch sphere, wherein the quantum state probabilities matrix comprises a plurality of probabilities representing:

a likelihood that a malicious actor moves between all potential combinations of categories of attack; and

a likelihood that the malicious actor uses a specific attack method of all of the categories of attack based on a previous category of attack; and

training a security threat model to perform a security threat classification based on the quantum state probabilities matrix, wherein the security threat classification infers a next category of attack against the security domain based on the previous category of attack.

21. The method of claim 20, further comprising performing the security threat classification of the security domain based on the quantum state probabilities matrix.