CLAIMS

WHAT IS CLAIMED IS:

1. A system comprising:

a non-transitory memory; and

one or more hardware processors coupled to the non-transitory memory and configured to read instructions from the non-transitory memory to cause the system to perform operations comprising:

receiving a plurality of signals associated with security behaviors of interest, wherein the plurality of signals correspond to a plurality of computing events occurring with a computing architecture corresponding to a service provider;

determining metadata for each of the plurality of signals based on a corresponding one of the plurality of computing events;

generating a plurality of vertices for entities corresponding to the plurality of signals in an *n*-dimensional space for a hypergraph;

connecting the plurality of vertices by at least one hyperedge in the *n*-dimensional space based on each of the plurality of signals shared by two or more of the entities;

generating the hypergraph based on the plurality of vertices and the at least one hyperedge; and

executing a search operation associated with a security threat of interest for one or more of the security behaviors of interest based on the hypergraph, wherein the search operation is based on a query identifying data associated at least one of the plurality of computing events, the metadata, or the entities.

2. The system of claim 1, wherein the operations further comprise:

generating a hypergraph data object for the hypergraph, wherein the hypergraph data object comprises identifiers for the plurality of signals and event hashes associated with the plurality of computing events for the metadata; and

storing the hypergraph data object in a searchable database accessible by a computing security system.

3. The system of claim 2, wherein the operations further comprise:

providing a search system for retrievals of security search result data from the hypergraph data object using a search option including at least one of the identifiers or the event hashes.

4. The system of claim 1, wherein the at least one hyperedge comprises at least one relationship between the two or more entities, and wherein each of the at least one relationship is correlated with a hash of an event object for each of the plurality of computing events.

5. The system of claim 1, wherein the search operation is associated with an identification of a scope of a computing activity associated with at least a portion of the plurality of signals.

6. The system of claim 1, wherein the search operation utilizes a hash associated with one of the plurality of computing events for a security investigation, and wherein the search operation requests identification of vertices related to the hash based on the at least one hyperedge.

7. The system of claim 1, wherein the search operation is associated with a creation of a threat-focused alert for a subset of the plurality of computing events linked by one of the at least one hyperedge.

8. The system of claim 1, wherein the metadata comprises at least one of an entity name, an entity identifier, a username, a host name, or an IP address from each of the plurality of computing events, and wherein the metadata further comprises a hash for each of the plurality of computing events calculated using a corresponding event log.

9. A method comprising:

receiving a plurality of signals associated with security behaviors of interest, wherein the plurality of signals correspond to a plurality of computing events occurring with a computing architecture corresponding to a service provider;

determining metadata for each of the plurality of signals based on a corresponding one of the plurality of computing events;

generating a plurality of vertices for entities corresponding to the plurality of signals in an *n*-dimensional space;

connecting the plurality of vertices by at least one hyperedge in the *n*-dimensional space based on each of the plurality of signals shared by two or more of the entities;

generating a hypergraph based on the plurality of vertices and the at least one hyperedge; and

executing a search operation associated with a security threat of interest for one or more of the security behaviors of interest based on the hypergraph, wherein the search operation is based on a query identifying data associated at least one of the plurality of computing events, the metadata, or the entities.

10. The method of claim 9, further comprising:

generating a hypergraph data object for the hypergraph, wherein the hypergraph data object comprises identifiers for the plurality of signals and event hashes associated with the plurality of computing events for the metadata;

storing the hypergraph data object in a searchable database accessible by a computing security system; and

providing a search system for retrievals of security search result data from the hypergraph data object using a search option including at least one of the identifiers or the event hashes.

11. The method of claim 9, wherein the at least one hyperedge comprises at least one relationship between the two or more entities, and wherein each of the at least one relationship is correlated with a hash of an event object for each of the plurality of computing events.

12. The method of claim 9, wherein the search operation is associated with an identification of a scope of a computing activity associated with at least a portion of the plurality of signals.

13. The method of claim 9, wherein the search operation utilizes a hash associated with one of the plurality of computing events for a security investigation, and wherein the search operation requests identification of vertices related to the hash based on the at least one hyperedge.

14. The method of claim 9, wherein the search operation is associated with a creation of a threat-focused alert for a subset of the plurality of computing events linked by one of the at least one hyperedge.

15. The method of claim 9, wherein the metadata comprises at least one of an entity name, an entity identifier, a username, a host name, or an IP address from each of the plurality of computing events, and wherein the metadata further comprises a hash for each of the plurality of computing events calculated using a corresponding event log.