

Listing of '627 Patent Challenged Claims

* within a given row, differences between claim elements are **bold-underlined**

Claim 1 & Dependents		Claim 11 & Dependents	
[1.1]	A computer system comprising:	[18.1]	A computer system comprising:
[1.2]	a hardware memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that:	[18.2]	a hardware memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that:
[1.3]	store in the hardware memory a representation of a first graph, wherein the representation of the first graph comprises representations of a first plurality of nodes corresponding to a first plurality of entities and further comprises representations of a first plurality of edges, wherein the first graph is a directed graph,	[18.3]	store in the hardware memory a representation of a first graph, wherein the representation of the first graph comprises representations of a first plurality of nodes corresponding to a first plurality of entities and further comprises representations of a first plurality of edges, wherein the first graph is a directed graph,
[1.4]	wherein the first plurality of entities comprises a plurality of accounts and a plurality of resources, and	[18.4]	wherein the first plurality of entities comprises a plurality of accounts and a plurality of resources, and
[1.5]	wherein each edge of the first plurality of edges corresponds to a respective relationship between a respective pair of entities;	[18.5]	wherein each edge of the first plurality of edges corresponds to a respective relationship between a respective pair of entities;
		[18.6]	identify, based on the representation of the first graph, a first plurality of attack paths comprising a first entity of the first plurality

			of entities, wherein each attack path of the first plurality of attack paths targets a second entity of the first plurality of entities,
[1.6]	receive streaming data comprising time-stamped data about events relating to one or more entities of the first plurality of entities,	[18.7]	receive streaming data comprising time-stamped data about events relating to one or more entities of the first plurality of entities,
[1.7]	based on a first portion of the streaming data, identify a <u>first</u> entity that does not correspond to any of the first plurality of nodes, wherein the <u>first</u> entity is not of the first plurality of entities,	[18.8]	based on a first portion of the streaming data, identify a <u>third</u> entity that does not correspond to any of the first plurality of nodes, wherein the <u>third</u> entity is not of the first plurality of entities,
[1.8]	based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges,	[18.9]	based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges,
[1.9]	modify, in the hardware memory, the representation of the first graph to generate a modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a <u>first node</u> corresponding to the <u>first</u> entity and <u>a representation of a first edge</u> corresponding to the first relationship, wherein the <u>first node</u> is not of the first	[18.10]	modify, in the hardware memory, the representation of the first graph to generate a modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a <u>node</u> corresponding to the <u>third</u> entity and <u>an edge</u> corresponding to the first relationship, wherein the <u>node</u> is not of the first plurality of nodes and the <u>edge</u> is not of the first plurality of edges, <u>and</u>

	plurality of nodes and the <u>first edge</u> is not of the first plurality of edges,		
[1.10]	identify, based on the modified representation of the first graph, <u>an attack path that could be involved in an attack involving the first entity,</u>	[18.11]	identify, based on the modified representation of the first graph, <u>a second plurality of attack paths comprising the first entity, wherein each attack path of the second plurality of attack paths targets the second entity, and wherein an attack path of the second plurality of attack paths comprises the third entity.</u>
[1.11]	wherein identifying the attack path comprises: identifying a second entity that can be reached using the first entity, wherein the second entity corresponds to a second node, and the second node is related by one or more edges to the first node corresponding to the first entity in the modified representation of the first graph; and, identifying a third entity that can be reached using the second entity, wherein the third entity corresponds to a third node, and the third node is related by one or more edges to the second node in the modified representation of the first graph; and		
[1.12]	generate a report comprising an identification of the first entity and at least one of the second entity and the third entity.		

2	The computer system of claim 1, wherein identifying the attack path further comprises: identifying a first plurality of event flows that include a first anomalous event associated with the first entity.	
3	The system of claim 2, wherein identifying the attack path further comprises: identifying a point of origin for the first anomalous event based on the first plurality of event flows.	
5	The computer system of claim 1, wherein the modified representation of the first graph comprises a representation of a node corresponding to the first entity, wherein the first entity is identified based on active reconnaissance results.	
6	The computer system of claim 1, wherein the modified representation of the first graph comprises a representation of a node corresponding to the first entity, wherein the first entity is identified based on passive reconnaissance results.	
11	The computer system of claim 1, wherein the computer system is further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that determine whether an event, of the events	

	relating to one or more entities of the first plurality of entities, is anomalous, wherein determining whether the event is anomalous comprises: determining that the event relates to the first entity, determining at least one behavior pattern associated with the first entity, and comparing the event to the at least one behavior pattern.	
12	The computer system of claim 11, wherein comparing the event to the at least one behavior pattern comprises using a threshold.	
13	The system of claim 11, wherein comparing the event to the at least one behavior pattern further comprises: determining that the first entity is associated with a resource, wherein the resource is a sensitive resource.	
14	The computer system of claim 1, wherein the computer system comprises a plurality of physical computing machines.	
16	The computer system of claim 1, wherein at least one entity of the first plurality of entities is at least one of a user, a place, a device, a resource, a group, or a service.	
17	The computer system of claim 1, wherein the representation of the first graph comprises a representation of at least one node that does not correspond to an entity.	

	22	The computer system of claim 18, wherein a portion of the representation of the first graph is derived from reconnaissance data received by the computer system from a plurality of computer systems, wherein a first computer system of the plurality of computer systems performs passive reconnaissance, and wherein a second computer system of the plurality of computer systems performs active reconnaissance.
	24	The computer system of claim 18, further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that analyze an attack path of the plurality of attack paths using a graph analysis algorithm.
	27	The computer system of claim 18, wherein the representation of the first graph comprises an identification of the third entity as a sensitive resource, and wherein the computer system is further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that generate a report that identifies the third entity as a sensitive resource.

	28	The computer system of claim 18, wherein the representation of the first graph comprises an identification of a security vulnerability associated with the third entity, and wherein an attack path of the second plurality of attack paths is based on the security vulnerability.
--	----	---