

Ex. F-1 - Invalidity of U.S. Patent No. 7,593,936 against U.S. Patent No. 7,225,343 to Honig et al. ("Honig")

Fortinet, Inc. ("Fortinet") provides this chart subject to all reservations, objections, statements, and disclaimers set forth herein and in Fortinet's Preliminary Invalidity Contentions Cover Pleading, as well as any amendment, supplement, or modification thereof, which are incorporated herein by reference in their entirety.

On information and belief, and subject to further investigation and discovery, Honig was filed on January 27, 2003, and is thus available as prior art under at least §102(e).

As illustrated in the chart below, Honig anticipates the asserted claims of the '936 Patent. To the extent the Honig is found not to expressly disclose certain limitations in the asserted claims, such limitations are inherent. To the extent the Honig is found not to anticipate any asserted claims or claim elements of the '936 Patent, the reference nevertheless renders those claims or claim elements obvious under 35 U.S.C. § 103, either alone or in combination with other art identified in the cover pleading or herein. These Preliminary Invalidity Contentions are not an admission by Fortinet that the accused products, including any current or past versions of the accused products, are covered by, or infringe the asserted claims, but are based instead on the recognition that if the claims are interpreted to be broad enough to encompass the accused products, the claims must also be construed to have that same scope when considering whether they are invalid.

The following chart is partially based on, but is not limited by, the claim constructions implicit in Plaintiff's Infringement Contentions, to the extent that such constructions are apparent from the Infringement Contentions. Fortinet notes that in many instances, Plaintiff's Infringement Contentions fail to provide adequate notice of Plaintiff's construction of the asserted claims and fail to comply with the Court's scheduling order and other applicable rules. Fortinet does not accept the assumptions concerning the scope and meaning implicit in Plaintiff's Infringement Contentions, to the extent those assumptions are discernible, and reserves the right to challenge Plaintiff's proposed (or implied) constructions. Fortinet also reserves the right to revise and supplement these charts if and when Plaintiff is permitted to provide revised Infringement Contentions or otherwise make its positions known. To the extent that these Preliminary Invalidity Contentions rely on or otherwise embody particular constructions of terms or phrases in the asserted claims, Fortinet does not necessarily advocate any such construction as proper constructions of those terms or phrase. Fortinet also reserves the right to revise and supplement these charts after the Court construes the claims. Citations given in the chart below are merely representative of the respective elements and are not meant to be exhaustive.

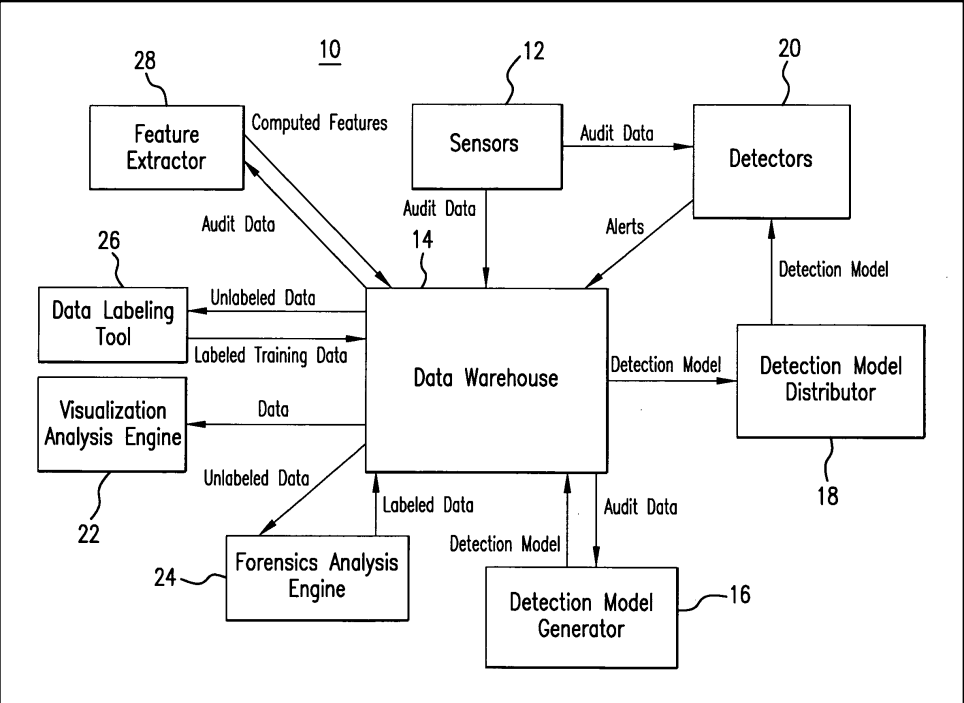
Claim	Exemplary Citation from Honig
[1PRE] A method of detecting abnormal system states in computers, comprising:	Honig discloses and/or renders obvious a method of detecting abnormal system states in computers with the following steps. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 16:25: "Forensics can be done with misuse detection models if there is a learned detection model for that data. If a learned detection model exists, it can be run over the data to find the intrusions in the data after the data has already been collected. The method can be applied with signature-based models which are used by commercial systems today. We can also use anomaly detection models if there exists a normal model for the data set. In some cases, there is no appropriate model to perform forensics. In these cases, an unsupervised anomaly detection algorithm may be used over the data. Unsupervised anomaly detection algorithms can be used to perform forensic analysis on unlabeled data. The adaptive model generation framework enables this process. Unsupervised anomaly detection algorithms detect intrusions buried within an unlabeled data set. Unsupervised anomaly detection algorithms are described in greater detail below."

Claim	Exemplary Citation from Honig
	Honig at Fig. 1 and corresponding text: <pre> graph TD 10[10] 12[12 Sensors] -- Audit Data --> 14[14 Data Warehouse] 28[28 Feature Extractor] -- Audit Data --> 14 28 -- Computed Features --> 14 26[26 Data Labeling Tool] -- Unlabeled Data --> 14 14 -- Labeled Training Data --> 26 22[22 Visualization Analysis Engine] -- Data --> 14 24[24 Forensics Analysis Engine] -- Unlabeled Data --> 14 14 -- Labeled Data --> 24 16[16 Detection Model Generator] -- Audit Data --> 14 14 -- Detection Model --> 16 14 -- Detection Model --> 18[18 Detection Model Distributor] 18 -- Detection Model --> 20[20 Detectors] 20 -- Alerts --> 14 14 -- Audit Data --> 20 </pre>
[1A] receiving snapshots from a plurality of computers within a population of computers, wherein individual snapshots include data indicating a state of a respective computer;	Honig discloses and/or renders obvious receiving snapshots from a plurality of computers within a population of computers, wherein individual snapshots include data indicating a state of a respective computer. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion

Claim	Exemplary Citation from Honig
	detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 5:61: "A system for detecting intrusions in the operation of a computer system is disclosed herein which comprises a plurality of sensors configured to gather information regarding the operation of the computer system, to format the information into data records having a predetermined format, and to transmit the data in the predetermined data format. A plurality of detection model generators may be configured to request data records from the data warehouse in the predetermined data format. Each detection model generator is configured to generate a respective intrusion detection model based on said data records, and to transmit the respective intrusion detection model to the data warehouse according to the predetermined data format. The invention provides a number of advantages, including the Support of heterogeneous data, a central storage of data at the data warehouse, and a common data format enables the system to combine data from different sources very easily. The distributed architecture of the adaptive model generation system allows machine learning algorithms use data from multiple sources just as easily as data from one Source. This allows correlation algorithms to be integrated into the adaptive model generation framework which could potentially increase the performance of an intrusion detection system. Accordingly, multiple different types of data Sources, and alert streams, can be algorithmically combined to detect a wider range of attacks, or even coordinated attacks targeting multiple sites. In accordance with the invention, the object described above have been met, and the need in the art for an effective intrusion detection architecture has been satisfied." Honig at 7:8: "More specifically, the system has the following major capabilities: Automated data collection is provided, in which data is collected by sensors and automatically sent to detectors for classification and to the data warehouse for aggregation and use in training models. Data warehousing capabilities is provided by a data warehouse component that stores data from all sensors. This data is used for

Claim	Exemplary Citation from Honig
	training detection models, but also may be used to Support various types of data analysis Such as forensic analysis. Automated model generation trains detection models from data stored in the data warehouse. The process for converting the data into the appropriate form for training is fully automated. Heterogeneous data Support permits the handling of data from different types of audit sources. This capability is allowed since any form of data can be represented using a general XML-based language." Honig at 8:14: "Sensors 12 gather information from an environment and send that data to the data warehouse 14. The data in the data warehouse 14 is accessed by the detection model generators 16 which generate models that classify activity as either malicious or normal. Once a model is created, it is stored in the data warehouse 14. A model distributor 18 deploys that model to a real-time detector 20. The detector 20 receives the detection model from the detection model distributor 18 and also receives the audit data from the sensor 12. Detector 20 then uses the model to evaluate the audit data from the sensor 12 to detect intrusions." Honig at 8:50: "The system 10 uses two basic components to provide real time detection capabilities: sensors 12 and detectors 20. A sensor 12 is a system that collects data from an audit stream and formats the data into the appropriate form using the XML markup language. This data is then sent to a detector 20 which uses a detection model to determine whether or not the data corresponds to an attack. If the data corresponds to an attack, the detector 20 generates an alert." Honig at 9:9: "The advantage of the system 10 over traditional system architectures is the integration of the sensors 12 and detectors 20 with other analysis and distribution sub-systems. In addition to sending the data to a detector 20, the sensor 12 also sends the data to a data warehouse 14 which aggregates and stores the data. The detector 20 retrieves its detection models from the model distributors 18. These detection models are created by other components of the system 10. Sensors 12 may be lightweight processes that gather information from a real-time audit stream, format the information into an XML representation, and then send the formatted data to the detectors 20 for real time intrusion detection and to the data warehouse 14 for aggregation of data and storage. The sensors 12 can gather

Claim	Exemplary Citation from Honig
	information from any source. For every different audit stream of data, a sensor 12 can be implemented to monitor and collect the data." Honig at 9:49: "In the exemplary embodiment, there are multiple sensors 12 for each host. This configuration may be implemented because there are several different streams of information that are useful for detecting intrusions. The system has been implemented with a variety of sensors for both WindowsTM and Linux systems. For a WindowsTM system, there are WindowsTM event log sensors, software wrappers, netatat sensors, and registry sensors. There are WindowsTM event log sensors which take information from the application, security, and event logs on the WindowsTM system respectively. Software wrappers are sensors that gather information about system calls. Netatat sensors use the netatat tool that gathers information about network connections on the hostdata. Registry sensors monitor the activity of the windows registry when applications are run on the host. The Linux sensors built into the system include process sensors, network connection sensors, resource sensors, and Software wrappers. Process sensors use the /proc virtual file-system to gather information about each running process. Network connection sensors collect information about network connections being made to and from the host machine. Resource sensors gather information about CPU and memory usage on a machine. The Software wrappers for Linux systems are the same as for WindowsTM, monitoring system calls made by a process." Honig at 12:35: "For example, if there are 40 WindowsTM hosts in a network, in order to create an anomaly detection model over the application Event logs for each of the hosts in the system framework, the following steps must be performed. A sensor 12 is installed on each of the hosts. This sensor collects the data and stores it in the data warehouse 14. If each host is typically used in the same way, a large data set may be created containing the combined event logs from each of the hosts." Honig at 25:29: "The second part of the RAD sensor is the communication component which translates this data into the XML format and sends it to the data warehouse 14. The communication module can support multiple BAMs at the same time. This is done so that all sensors running on a host can be sent

Claim	Exemplary Citation from Honig
	through a single source. Then the communication engine can send the data from all these sources to the data warehouse for storage." Honig at 26:11: "The multiplicity of this system can easily be increased with the novel system described herein. With no changes in architecture, the system can Support any number of host machines and sensors. With a conventional system architecture, increasing the multiplicity would require major changes in the structure of a system. According to the invention, the central data collection is automated in the system. This means that data from multiple machines is gathered in the same place and can be analyzed from that central location." Honig at Fig. 1 and corresponding text:  <pre> graph TD 10[10] --- 12[12 Sensors] 12 -- Audit Data --> 14[14 Data Warehouse] 28[28 Feature Extractor] -- Audit Data --> 14 28 -- Computed Features --> 14 26[26 Data Labeling Tool] -- Unlabeled Data --> 14 14 -- Labeled Training Data --> 26 22[22 Visualization Analysis Engine] -- Data --> 14 24[24 Forensics Analysis Engine] -- Unlabeled Data --> 14 14 -- Labeled Data --> 24 16[16 Detection Model Generator] -- Detection Model --> 14 14 -- Audit Data --> 16 14 -- Detection Model --> 18[18 Detection Model Distributor] 18 -- Detection Model --> 20[20 Detectors] 20 -- Alerts --> 14 </pre>

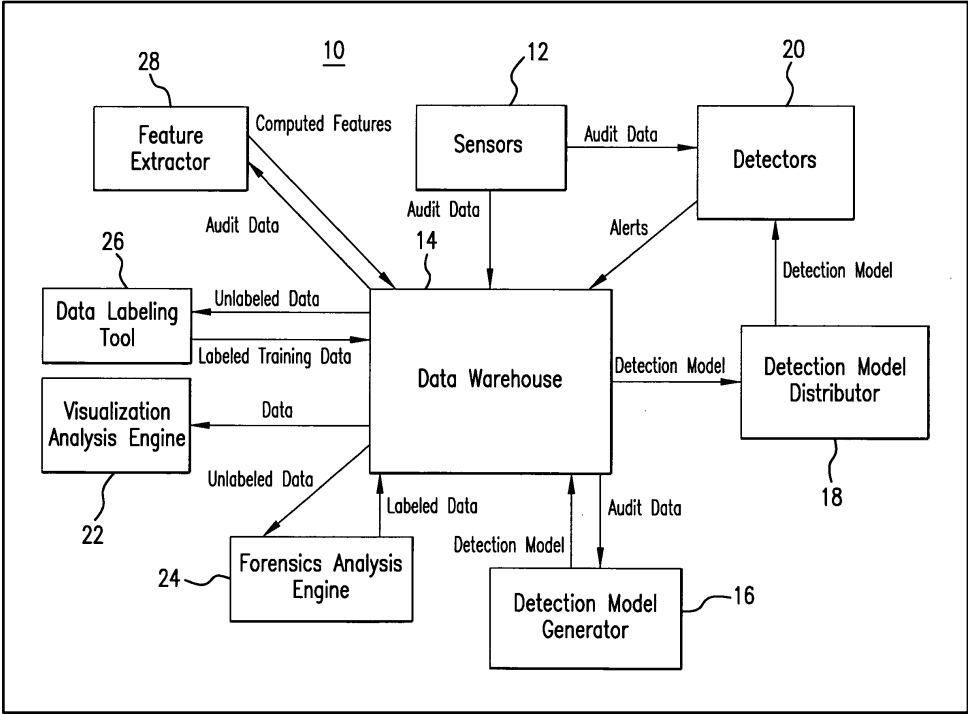
Claim	Exemplary Citation from Honig
[1B] automatically generating an adaptive reference model comprising a rule set customized to characteristics of the population of computers, the rule set being developed by identifying patterns among the snapshots from the plurality of computers such that the adaptive reference model is indicative of normal states in the computers within the population; and	Honig discloses and/or renders obvious automatically generating an adaptive reference model comprising a rule set customized to characteristics of the population of computers, the rule set being developed by identifying patterns among the snapshots from the plurality of computers such that the adaptive reference model is indicative of normal states in the computers within the population. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 5:61: "A system for detecting intrusions in the operation of a computer system is disclosed herein which comprises a plurality of sensors configured to gather information regarding the operation of the computer system, to format the information into data records having a predetermined format, and to transmit the data in the predetermined data format. A plurality of detection model generators may be configured to request data records from the data warehouse in the predetermined data format. Each detection model generator is configured to generate a respective intrusion detection model based on said data records, and to transmit the respective intrusion detection model to the data warehouse according to the predetermined data format. The invention provides a number of advantages, including the Support of heterogeneous data, a central storage of data at the data warehouse, and a common data format enables the system to combine data from different sources very easily. The distributed architecture of the adaptive model generation system allows machine learning algorithms

Claim	Exemplary Citation from Honig
	use data from multiple sources just as easily as data from one Source. This allows correlation algorithms to be integrated into the adaptive model generation framework which could potentially increase the performance of an intrusion detection system. Accordingly, multiple different types of data Sources, and alert streams, can be algorithmically combined to detect a wider range of attacks, or even coordinated attacks targeting multiple sites. In accordance with the invention, the object described above have been met, and the need in the art for an effective intrusion detection architecture has been satisfied." Honig at 6:50: "The system in accordance with the present invention (also referred to as "Adaptive Model Generation' or AMG) is an architecture which provides and automates many of the critical processes in the deployment and operation of real time data mining-based intrusion detection systems. The system abstracts various parts of the data mining-based IDS process and formalizes the automation of this process. This includes abstracting the processes of data collection, data aggregation, detection model evaluation, detection model generation, and model distribution. The system uses a general XML-based data and model representation scheme that facilitates the translation of data from what is collected at the audit stream to the form necessary for generation of detection models." Honig at 7:8: "More specifically, the system has the following major capabilities: Automated data collection is provided, in which data is collected by sensors and automatically sent to detectors for classification and to the data warehouse for aggregation and use in training models. Data warehousing capabilities is provided by a data warehouse component that stores data from all sensors. This data is used for training detection models, but also may be used to Support various types of data analysis Such as forensic analysis. Automated model generation trains detection models from data stored in the data warehouse. The process for converting the data into the appropriate form for training is fully automated. Heterogeneous data Support permits the handling of data from different types of audit sources. This capability is allowed since any form of data can be represented using a general XML-based language."

Claim	Exemplary Citation from Honig
	Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 11:56: "Detectors 20 receive detection models from model distributors 18, which distribute models stored in the data warehouse originally created by model generators. The detectors 20 receive real time updates from the model distributors 18. This process keeps the detection models updated as soon as new models are available. Below is an example of a model that the detector 20 for the RAD system (described below and in U.S. application Ser. No. 10/352. 343 concurrently filed, entitled "System and Methods for Detecting Intrusions in a Computer System by Monitoring Operating System Registry Accesses," uses to make a classification." Honig at 12:17: "The data warehouse 14 is described herein. It serves as the central storage repository for all of the data collected by the sensors 12. The model generators 16 access the data in the data warehouse 14 and create detection models using this data. The data warehouse 14 also stores these detection

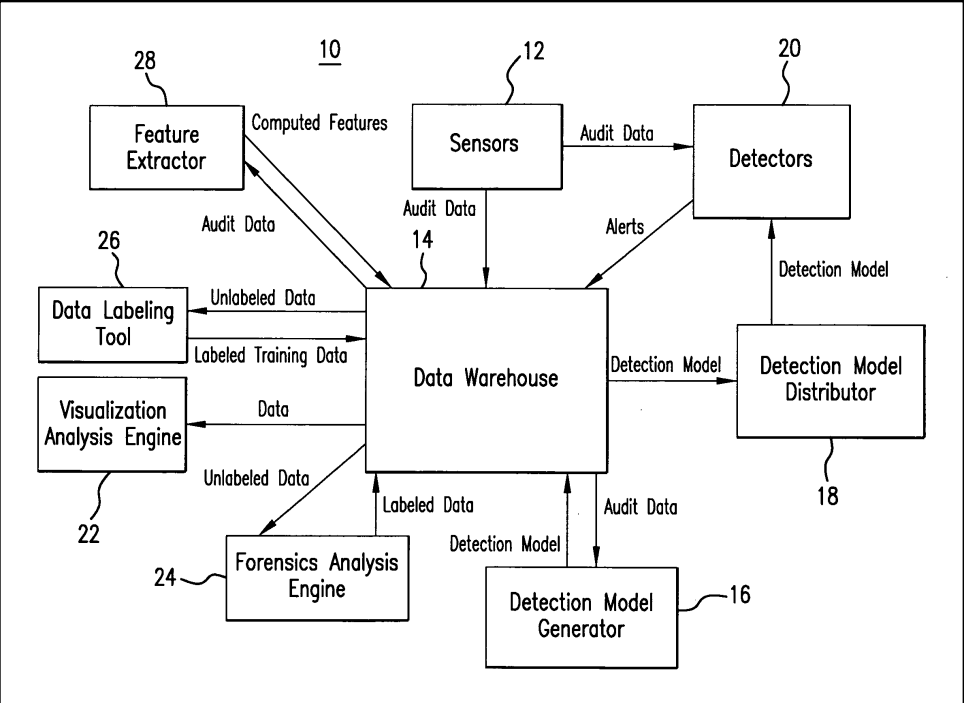
Claim	Exemplary Citation from Honig
	models. The analysis engines 22, 24, 26, and 28 also access the data stored in the data warehouse 14." Honig at 12:35: "For example, if there are 40 WindowsTM hosts in a network, in order to create an anomaly detection model over the application Event logs for each of the hosts in the system framework, the following steps must be performed. A sensor 12 is installed on each of the hosts. This sensor collects the data and stores it in the data warehouse 14. If each host is typically used in the same way, a large data set may be created containing the combined event logs from each of the hosts." Honig at 13:56: "The system 10 manages the creation and distribution of detection models. The detection models are generated by the detection model generators 16 using data collected stored in the data warehouse 14. They are distributed to the detectors 20 by the model distributors 18, as described herein." Honig at 14:5: "The model generation modules 16 request the data from the data warehouse 14 when they want to create a model. They form their request based on the information that the model needs to train on. The generator 16 then runs and creates a model. This model is then encoded into XML and sent to the data warehouse 14. Model generators 16 also signal the model distributor 18 to let it know that a new model is available. A sample XML encoding of a model generated by the RAD system is shown below." Honig at 19:32: "The distributed architecture of system 10 allows the system to gather data from heterogeneous systems. A set of standard guidelines in a flexible format are placed on sensor data, as described in the Appendix. There are many different types of information that IDSs use, such as e.g., network packets, application logs, WindowsTM registry accesses, etc. The ability to accommodate these different sources of information in a consistent way is a large advantage of the adaptive model generation system."

Claim	Exemplary Citation from Honig
	Honig at 20:32: "There are three exemplary types of model generation algorithms that the system 10 supports. The first is misuse detection, which trains on labeled normal and attack data. The second is Supervised (traditional) anomaly detection which trains on normal data. The third is unsupervised anomaly detection which trains on unlabeled data." Honig at 21:13: "The adaptive model generation framework Supports the creation of anomaly detection models. Since sensors send data to the data warehouse, it is easy to aggregate the data for collection. Using the forensics analysis engine, it is possible to see if the data is clean and contains no intrusions. This can greatly decrease the cost of creating the training set since it speeds the process of Verifying that the data is clean. The model generators can automatically generate anomaly detection models using the data from the data warehouse and deploy the detection models using the model distributor. Unsupervised anomaly detection algorithms examine unlabeled data and attempt to detect intrusions buried within the unlabeled data. Unsupervised anomaly detection algorithms operate under the principle that intrusions are very rare compared to the normal data and they are also quantitatively different. Because of this, intrusions are outliers in the data and can be detected. Since unsupervised anomaly detection can detect intrusions in an unlabeled data set, they are used inside the forensics analysis engines. Data from the data warehouse is sent to a forensics analysis engine where an unsupervised anomaly detection algorithm is applied. The forensics analysis engine can label the data which it determines to be an outlier. Unsupervised anomaly detection algorithms can also be used to help label data that is collected by the system. This labeled data can then be used to train a misuse or anomaly detection model." Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of

Claim	Exemplary Citation from Honig
	normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20." Honig at 26:11: "The multiplicity of this system can easily be increased with the novel system described herein. With no changes in architecture, the system can Support any number of host machines and sensors. With a conventional system architecture, increasing the multiplicity would require major changes in the structure of a system. According to the invention, the central data collection is automated in the system. This means that data from multiple machines is gathered in the same place and can be analyzed from that central location." Honig at Fig. 1 and corresponding text:  <pre> graph TD 10[10] --- 12[12] 10 --- 20[20] 10 --- 28[28] 10 --- 26[26] 10 --- 22[22] 10 --- 24[24] 10 --- 14[14] 12 -- Audit Data --> 14 14 -- Audit Data --> 28 14 -- Audit Data --> 26 14 -- Audit Data --> 22 14 -- Audit Data --> 24 14 -- Audit Data --> 20 14 -- Audit Data --> 16 28 -- Computed Features --> 14 26 -- Unlabeled Data --> 14 26 -- Labeled Training Data --> 28 22 -- Data --> 14 24 -- Labeled Data --> 14 14 -- Detection Model --> 16 16 -- Detection Model --> 14 16 -- Detection Model --> 18 18 -- Detection Model --> 20 20 -- Alerts --> 14 </pre>

Claim	Exemplary Citation from Honig
[1C] comparing a snapshot from at least one of the computers to the adaptive reference model to determine whether an anomaly is present in the state of the at least one of the computers.	<i>See also</i> Honig at 11:8-55, 20:39-27:57. Honig discloses and/or renders obvious comparing a snapshot from at least one of the computers to the adaptive reference model to determine whether an anomaly is present in the state of the at least one of the computers. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they

Claim	Exemplary Citation from Honig
	coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 8:50: "The system 10 uses two basic components to provide real time detection capabilities: sensors 12 and detectors 20. A sensor 12 is a system that collects data from an audit stream and formats the data into the appropriate form using the XML markup language. This data is then sent to a detector 20 which uses a detection model to determine whether or not the data corresponds to an attack. If the data corresponds to an attack, the detector 20 generates an alert." Honig at 11:8: "Detectors 20 analyze audit stream data collected from a sensor and detect intrusions by using a detection model. A detector 20 performs model evaluation over each record from the sensor. The way a specific detector works depends on the type of model being evaluated. Each different model type may have a different detector that implements model evaluation for that model type. The detector 20 may be viewed as a function that takes as input a data record and outputs an alert if the data is determined to correspond to an intrusion. An example of a detection model type is a signature-based model, which is the algorithm most widely used in commercial intrusion detection systems. A signature-based detection model simply contains a set of 'signatures' which correspond to known attack types. Model evaluation consists of matching each signature in the model to a data record. If any of the signatures match, the detector generates an alert." Honig at 11:47: "The detector would effectively map a record to this high dimensional feature space and computes which side of the decision boundary the record falls on to determine whether or not to generate an alert. Further details on the Support vector machine model generation and detection are provided below and in U.S. application Ser. No. 10/320.259, filed Dec. 16, 2002, entitled "Methods of Unsupervised Anomaly Detection Using a Geometric Framework," which is incorporated by reference in its entirety herein."

Claim	Exemplary Citation from Honig
	Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20." Honig at Fig. 1 and corresponding text:  <pre> graph TD 10[10] 12[Sensors 12] -- Audit Data --> 14[Data Warehouse 14] 14 -- Audit Data --> 28[Feature Extractor 28] 28 -- Computed Features --> 14 14 -- Audit Data --> 16[Detection Model Generator 16] 16 -- Detection Model --> 14 14 -- Audit Data --> 18[Detection Model Distributor 18] 18 -- Detection Model --> 20[Detectors 20] 20 -- Alerts --> 14 14 -- Labeled Training Data --> 26[Data Labeling Tool 26] 26 -- Unlabeled Data --> 14 14 -- Data --> 22[Visualization Analysis Engine 22] 22 -- Unlabeled Data --> 14 14 -- Labeled Data --> 24[Forensics Analysis Engine 24] 24 -- Labeled Data --> 14 </pre>

Claim	Exemplary Citation from Honig
[2PRE] The method of claim 1, further comprising:	<i>See claim 1.</i>
[2A] comparing the anomaly to a recognition filter to diagnose a trouble condition on the at least one of the computers; and	Honig discloses and/or renders obvious comparing the anomaly to a recognition filter to diagnose a trouble condition on the at least one of the computers. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they

Claim	Exemplary Citation from Honig
	coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 8:50: "The system 10 uses two basic components to provide real time detection capabilities: sensors 12 and detectors 20. A sensor 12 is a system that collects data from an audit stream and formats the data into the appropriate form using the XML markup language. This data is then sent to a detector 20 which uses a detection model to determine whether or not the data corresponds to an attack. If the data corresponds to an attack, the detector 20 generates an alert." Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20."

Claim	Exemplary Citation from Honig
	Honig at Fig. 1 and corresponding text: <pre> graph TD 10[10] --- 12[12 Sensors] 12 -- Audit Data --> 14[14 Data Warehouse] 14 -- Audit Data --> 28[28 Feature Extractor] 14 -- Audit Data --> 24[24 Forensics Analysis Engine] 28 -- Computed Features --> 14 14 -- Unlabeled Data --> 26[26 Data Labeling Tool] 14 -- Unlabeled Data --> 22[22 Visualization Analysis Engine] 26 -- Labeled Training Data --> 14 22 -- Data --> 14 14 -- Labeled Data --> 24 14 -- Audit Data --> 16[16 Detection Model Generator] 16 -- Detection Model --> 14 14 -- Detection Model --> 18[18 Detection Model Distributor] 18 -- Detection Model --> 20[20 Detectors] 20 -- Alerts --> 14 14 -- Audit Data --> 20 </pre>
[2B] in the event of a trouble condition, generating an automated response to the trouble condition.	Honig discloses and/or renders obvious, in the event of a trouble condition, generating an automated response to the trouble condition. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is

Claim	Exemplary Citation from Honig
	configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 8:50: "The system 10 uses two basic components to provide real time detection capabilities: sensors 12 and detectors 20. A sensor 12 is a system that collects data from an audit stream and formats the data into the appropriate form using the XML markup language. This data is then sent to a detector 20 which uses a detection model to determine whether or not the data corresponds to an attack. If the data corresponds to an attack, the detector 20 generates an alert."

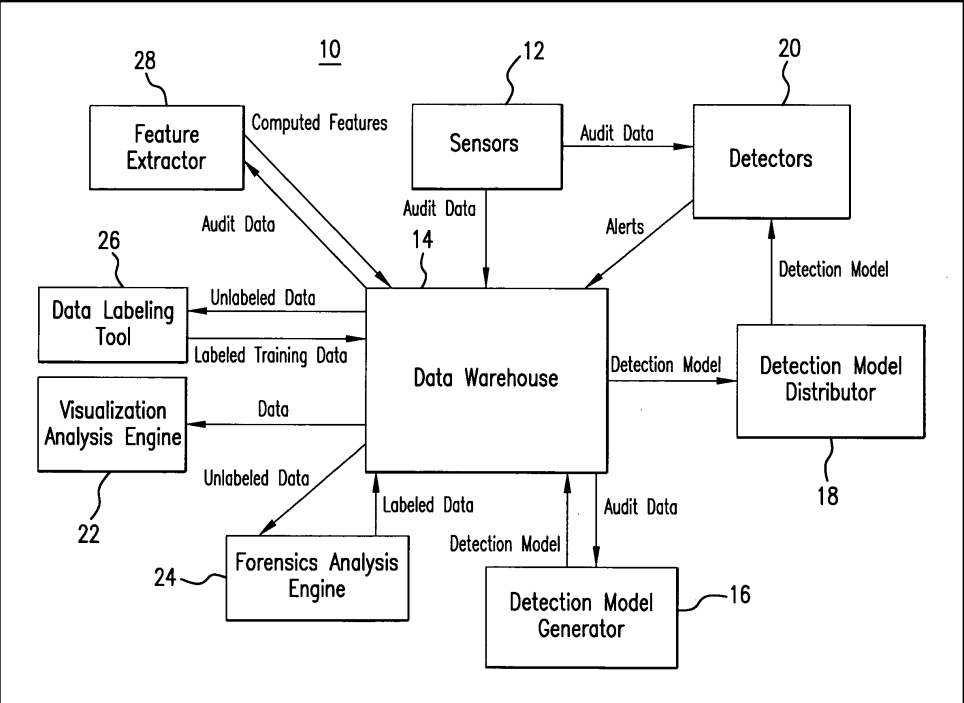
Claim	Exemplary Citation from Honig
	Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20." Honig at Fig. 1 and corresponding text: <pre> graph TD 10[10] --- 12[Sensors 12] 12 -- "Audit Data" --> 14[Data Warehouse 14] 14 -- "Alerts" --> 20[Detectors 20] 20 -- "Detection Model" --> 18[Detection Model Distributor 18] 18 -- "Detection Model" --> 16[Detection Model Generator 16] 16 -- "Detection Model" --> 14 14 -- "Labeled Data" --> 16 14 -- "Unlabeled Data" --> 26[Data Labeling Tool 26] 26 -- "Labeled Training Data" --> 14 14 -- "Data" --> 22[Visualization Analysis Engine 22] 14 -- "Unlabeled Data" --> 24[Forensics Analysis Engine 24] 28[Feature Extractor 28] -- "Computed Features" --> 14 14 -- "Audit Data" --> 28 </pre>

Claim	Exemplary Citation from Honig
[3PRE] The method of claim 2, wherein the automated response is a generic response not specific to a particular asset of the at least one computer, and wherein the method further comprises:	Honig discloses and/or renders obvious that the automated response is a generic response not specific to a particular asset of the at least one computer. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high

Claim	Exemplary Citation from Honig
	bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 8:50: "The system 10 uses two basic components to provide real time detection capabilities: sensors 12 and detectors 20. A sensor 12 is a system that collects data from an audit stream and formats the data into the appropriate form using the XML markup language. This data is then sent to a detector 20 which uses a detection model to determine whether or not the data corresponds to an attack. If the data corresponds to an attack, the detector 20 generates an alert." Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20."

Claim	Exemplary Citation from Honig
	Honig at Fig. 1 and corresponding text: <pre> graph TD 10[10] --- 12[12 Sensors] 12 -- Audit Data --> 14[14 Data Warehouse] 14 -- Audit Data --> 28[28 Feature Extractor] 28 -- Computed Features --> 14 14 -- Audit Data --> 20[20 Detectors] 14 -- Alerts --> 20 20 -- Audit Data --> 14 14 -- Unlabeled Data --> 26[26 Data Labeling Tool] 26 -- Labeled Training Data --> 14 14 -- Data --> 22[22 Visualization Analysis Engine] 14 -- Unlabeled Data --> 24[24 Forensics Analysis Engine] 14 -- Labeled Data --> 16[16 Detection Model Generator] 16 -- Detection Model --> 14 14 -- Detection Model --> 18[18 Detection Model Distributor] 18 -- Detection Model --> 20 </pre>
[3A] sending the generic response and a set of anomalies found in the snapshot to the at least one computer, the set of anomalies indicating assets of the at least one computer whose states are anomalous; and	Honig discloses and/or renders obvious sending the generic response and a set of anomalies found in the snapshot to the at least one computer, the set of anomalies indicating assets of the at least one computer whose states are anomalous. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion

Claim	Exemplary Citation from Honig
	detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 8:50: "The system 10 uses two basic components to provide real time detection capabilities: sensors 12 and detectors 20. A sensor 12 is a system that collects data from an audit stream and formats the data into the appropriate form using the XML markup language. This data is then sent to a detector 20 which uses a detection model to determine whether or not the data corresponds to an attack. If the data corresponds to an attack, the detector 20 generates an alert."

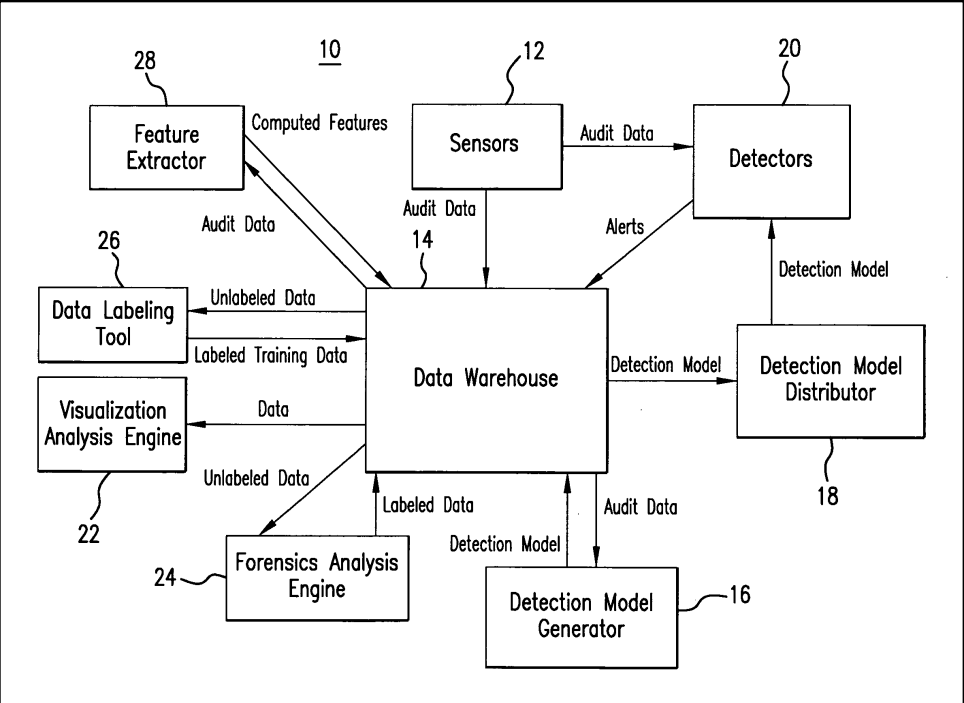
Claim	Exemplary Citation from Honig
	Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20." Honig at Fig. 1 and corresponding text:  <pre> graph TD Sensors[12] -- Audit Data --> DW[14] DW -- Alerts --> Detectors[20] Detectors -- Detection Model --> DMD[18] DMD -- Detection Model --> DW DW -- Labeled Data --> DMG[16] DMG -- Audit Data --> DW DW -- Unlabeled Data --> DLT[26] DLT -- Labeled Training Data --> DW DW -- Data --> VAE[22] VAE -- Unlabeled Data --> DW DW -- Unlabeled Data --> FAE[24] FAE -- Labeled Data --> DW DW -- Computed Features --> FE[28] FE -- Audit Data --> DW </pre>

Claim	Exemplary Citation from Honig
[3B] applying the generic response to the anomalous assets to correct the trouble condition.	Honig discloses and/or renders obvious applying the generic response to the anomalous assets to correct the trouble condition. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high

Claim	Exemplary Citation from Honig
	bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 8:50: "The system 10 uses two basic components to provide real time detection capabilities: sensors 12 and detectors 20. A sensor 12 is a system that collects data from an audit stream and formats the data into the appropriate form using the XML markup language. This data is then sent to a detector 20 which uses a detection model to determine whether or not the data corresponds to an attack. If the data corresponds to an attack, the detector 20 generates an alert." Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20."

Claim	Exemplary Citation from Honig
	Honig at Fig. 1 and corresponding text: <pre> graph TD 10[10] 12[12 Sensors] -- Audit Data --> 14[14 Data Warehouse] 14 -- Audit Data --> 28[28 Feature Extractor] 28 -- Computed Features --> 14 14 -- Audit Data --> 20[20 Detectors] 20 -- Alerts --> 14 20 -- Audit Data --> 14 14 -- Unlabeled Data --> 26[26 Data Labeling Tool] 26 -- Labeled Training Data --> 14 14 -- Data --> 22[22 Visualization Analysis Engine] 14 -- Unlabeled Data --> 24[24 Forensics Analysis Engine] 14 -- Labeled Data --> 16[16 Detection Model Generator] 16 -- Detection Model --> 14 14 -- Detection Model --> 18[18 Detection Model Distributor] 18 -- Detection Model --> 20 </pre>
[4] The method of claim 3, wherein the generic response includes at least one of: installing a missing software component, removing an undesirable software component, and restoring an incorrect registry setting.	Honig discloses and/or renders obvious that the generic response includes at least one of: installing a missing software component, removing an undesirable software component, and restoring an incorrect registry setting. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion

Claim	Exemplary Citation from Honig
	detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 8:50: "The system 10 uses two basic components to provide real time detection capabilities: sensors 12 and detectors 20. A sensor 12 is a system that collects data from an audit stream and formats the data into the appropriate form using the XML markup language. This data is then sent to a detector 20 which uses a detection model to determine whether or not the data corresponds to an attack. If the data corresponds to an attack, the detector 20 generates an alert."

Claim	Exemplary Citation from Honig
	Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20." Honig at Fig. 1 and corresponding text:  <pre> graph TD 10[10] 12[Sensors 12] -- Audit Data --> 14[Data Warehouse 14] 14 -- Audit Data --> 28[Feature Extractor 28] 28 -- Computed Features --> 14 14 -- Audit Data --> 16[Detection Model Generator 16] 16 -- Labeled Data --> 14 14 -- Unlabeled Data --> 26[Data Labeling Tool 26] 26 -- Labeled Training Data --> 14 14 -- Data --> 22[Visualization Analysis Engine 22] 22 -- Unlabeled Data --> 14 14 -- Labeled Data --> 24[Forensics Analysis Engine 24] 24 -- Unlabeled Data --> 14 14 -- Audit Data --> 18[Detection Model Distributor 18] 18 -- Detection Model --> 20[Detectors 20] 20 -- Alerts --> 14 </pre>

Claim	Exemplary Citation from Honig
[5] The method of claim 2, wherein the recognition filter comprises a particular pattern of anomalies that indicates the presence of a particular root cause condition or a generic class of conditions.	Honig discloses and/or renders obvious that the recognition filter comprises a particular pattern of anomalies that indicates the presence of a particular root cause condition or a generic class of conditions. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected

Claim	Exemplary Citation from Honig
	LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 8:50: "The system 10 uses two basic components to provide real time detection capabilities: sensors 12 and detectors 20. A sensor 12 is a system that collects data from an audit stream and formats the data into the appropriate form using the XML markup language. This data is then sent to a detector 20 which uses a detection model to determine whether or not the data corresponds to an attack. If the data corresponds to an attack, the detector 20 generates an alert." Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20."

Claim	Exemplary Citation from Honig
	Honig at Fig. 1 and corresponding text:
[6PRE] The method of claim 1, further comprising:	See Claim 1.
[6A] comparing a plurality of anomalies associated with a particular snapshot with a recognition filter to diagnose a trouble condition; and	Honig discloses and/or renders obvious comparing a plurality of anomalies associated with a particular snapshot with a recognition filter to diagnose a trouble condition. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to

Claim	Exemplary Citation from Honig
	generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 8:50: "The system 10 uses two basic components to provide real time detection capabilities: sensors 12 and detectors 20. A sensor 12 is a system that collects data from an audit stream and formats the data into the appropriate form using the XML markup language. This data is then sent to a detector 20 which uses a detection model to determine whether or not the data corresponds to an attack. If the data corresponds to an attack, the detector 20 generates an alert."

Claim	Exemplary Citation from Honig
	Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20." Honig at Fig. 1 and corresponding text: <pre> graph TD 10[10] 12[Sensors 12] -- Audit Data --> 14[Data Warehouse 14] 14 -- Audit Data --> 20[Detectors 20] 14 -- Audit Data --> 16[Detection Model Generator 16] 14 -- Labeled Data --> 16 14 -- Unlabeled Data --> 26[Data Labeling Tool 26] 14 -- Unlabeled Data --> 24[Forensics Analysis Engine 24] 26 -- Labeled Training Data --> 14 24 -- Labeled Data --> 14 14 -- Data --> 22[Visualization Analysis Engine 22] 14 -- Detection Model --> 18[Detection Model Distributor 18] 18 -- Detection Model --> 20 20 -- Alerts --> 14 28[Feature Extractor 28] -- Computed Features --> 14 14 -- Audit Data --> 28 </pre>

Claim	Exemplary Citation from Honig
[6B] diagnosing a trouble condition on the at least one of the computers in response to at least a subset of the plurality of anomalies matching information in the recognition filter.	Honig discloses and/or renders obvious diagnosing a trouble condition on the at least one of the computers in response to at least a subset of the plurality of anomalies matching information in the recognition filter. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected

Claim	Exemplary Citation from Honig
	LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 8:50: "The system 10 uses two basic components to provide real time detection capabilities: sensors 12 and detectors 20. A sensor 12 is a system that collects data from an audit stream and formats the data into the appropriate form using the XML markup language. This data is then sent to a detector 20 which uses a detection model to determine whether or not the data corresponds to an attack. If the data corresponds to an attack, the detector 20 generates an alert." Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20."

Claim	Exemplary Citation from Honig
	Honig at Fig. 1 and corresponding text: <pre> graph TD 10[10] 12[Sensors 12] -- Audit Data --> 14[Data Warehouse 14] 28[Feature Extractor 28] -- Audit Data --> 14 28 -- Computed Features --> 14 26[Data Labeling Tool 26] -- Unlabeled Data --> 14 14 -- Labeled Training Data --> 26 22[Visualization Analysis Engine 22] -- Data --> 14 24[Forensics Analysis Engine 24] -- Unlabeled Data --> 14 14 -- Labeled Data --> 24 16[Detection Model Generator 16] -- Audit Data --> 14 16 -- Detection Model --> 18[Detection Model Distributor 18] 18 -- Detection Model --> 20[Detectors 20] 20 -- Alerts --> 14 </pre>
[7] The method of claim 1, wherein individual snapshots include data associated with at least one of: system files, application files, a registry entry, a performance counter, a process, a communication port, a hardware configuration, a log file, a running task, services, and network connections.	Honig discloses and/or renders obvious that individual snapshots include data associated with at least one of: system files, application files, a registry entry, a performance counter, a process, a communication port, a hardware configuration, a log file, a running task, services, and network connections. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to

Claim	Exemplary Citation from Honig
	generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 5:61: "A system for detecting intrusions in the operation of a computer system is disclosed herein which comprises a plurality of sensors configured to gather information regarding the operation of the computer system, to format the information into data records having a predetermined format, and to transmit the data in the predetermined data format. A plurality of detection model generators may be configured to request data records from the data warehouse in the predetermined data format. Each detection model generator is configured to generate a respective intrusion detection model based on said data records, and to transmit the respective intrusion detection model to the data warehouse according to the predetermined data format. The invention provides a number of advantages, including the Support of heterogeneous data, a central storage of data at the data warehouse, and a common data format enables the system to combine data from different sources very easily. The distributed architecture of the adaptive model generation system allows machine learning algorithms use data from multiple sources just as easily as data from one Source. This allows correlation algorithms to be integrated into the adaptive model generation framework which could potentially increase the performance of an intrusion detection system. Accordingly, multiple different types of data Sources, and alert streams, can be algorithmically combined to detect a wider range of attacks, or even coordinated attacks targeting multiple sites. In accordance with the invention, the object described above have been met, and the need in the art for an effective intrusion detection architecture has been satisfied." Honig at 7:8: "More specifically, the system has the following major capabilities: Automated data collection is provided, in which data is collected by sensors and automatically sent to detectors for classification and to the data warehouse for aggregation and use in training models. Data warehousing capabilities

Claim	Exemplary Citation from Honig
	is provided by a data warehouse component that stores data from all sensors. This data is used for training detection models, but also may be used to Support various types of data analysis Such as forensic analysis. Automated model generation trains detection models from data stored in the data warehouse. The process for converting the data into the appropriate form for training is fully automated. Heterogeneous data Support permits the handling of data from different types of audit sources. This capability is allowed since any form of data can be represented using a general XML-based language." Honig at 8:50: "The system 10 uses two basic components to provide real time detection capabilities: sensors 12 and detectors 20. A sensor 12 is a system that collects data from an audit stream and formats the data into the appropriate form using the XML markup language. This data is then sent to a detector 20 which uses a detection model to determine whether or not the data corresponds to an attack. If the data corresponds to an attack, the detector 20 generates an alert." Honig at 9:49: "In the exemplary embodiment, there are multiple sensors 12 for each host. This configuration may be implemented because there are several different streams of information that are useful for detecting intrusions. The system has been implemented with a variety of sensors for both WindowsTM and Linux systems. For a WindowsTM system, there are WindowsTM event log sensors, software wrappers, netatat sensors, and registry sensors. There are WindowsTM event log sensors which take information from the application, security, and event logs on the WindowsTM system respectively. Software wrappers are sensors that gather information about system calls. Netatat sensors use the netatat tool that gathers information about network connections on the hostdata. Registry sensors monitor the activity of the windows registry when applications are run on the host. The Linux sensors built into the system include process sensors, network connection sensors, resource sensors, and Software wrappers. Process sensors use the /proc virtual file-system to gather information about each running process. Network connection sensors collect information about network connections being made to and from the host machine. Resource sensors gather information about CPU and memory usage on a machine. The Software wrappers for Linux systems are the same as for WindowsTM, monitoring system calls made by a process."

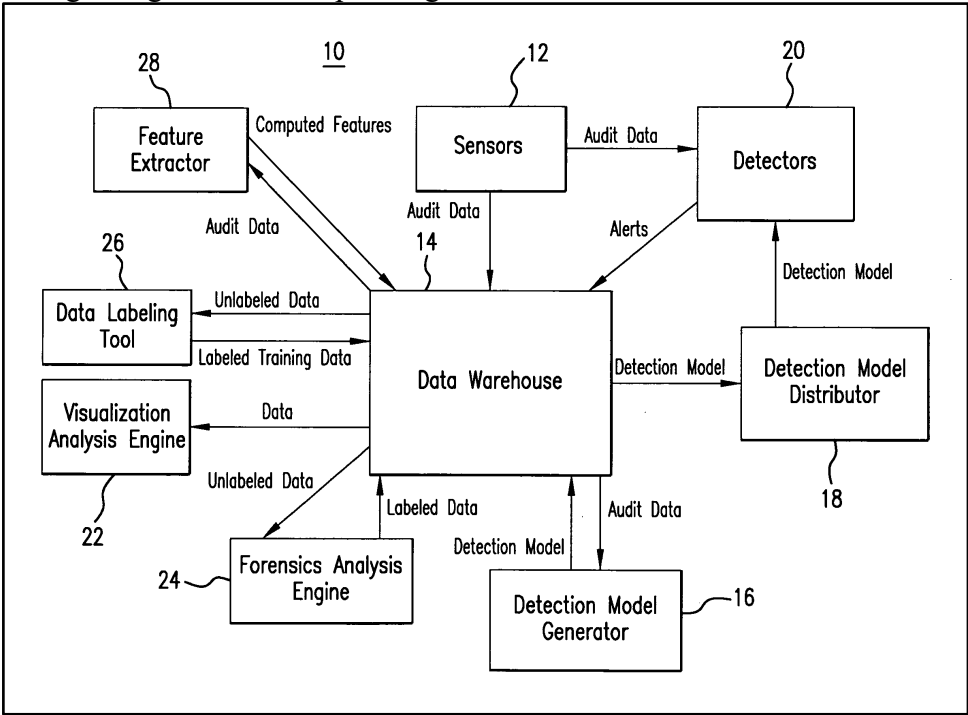
Claim	Exemplary Citation from Honig
	Honig at 12:35: "For example, if there are 40 Windows™ hosts in a network, in order to create an anomaly detection model over the application Event logs for each of the hosts in the system framework, the following steps must be performed. A sensor 12 is installed on each of the hosts. This sensor collects the data and stores it in the data warehouse 14. If each host is typically used in the same way, a large data set may be created containing the combined event logs from each of the hosts." Honig at Fig. 1 and corresponding text:
[8] The method of claim 1, further comprising: inserting rules into the rule set of the adaptive reference model to augment or	Honig discloses and/or renders obvious inserting rules into the rule set of the adaptive reference model to augment or override rules of the rule set automatically generated from the snapshots. Honig at Abstract:

Claim	Exemplary Citation from Honig
override rules of the rule set automatically generated from the snapshots.	"A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 5:61: "A system for detecting intrusions in the operation of a computer system is disclosed herein which comprises a plurality of sensors configured to gather information regarding the operation of the computer system, to format the information into data records having a predetermined format, and to transmit the data in the predetermined data format. A plurality of detection model generators may be configured to request data records from the data warehouse in the predetermined data format. Each detection model generator is configured to generate a respective intrusion detection model based on said data records, and to transmit the respective intrusion detection model to the data warehouse according to the predetermined data format. The invention provides a number of advantages, including the Support of heterogeneous data, a central storage of data at the data warehouse, and a common data format enables the system to combine data from different sources very easily. The distributed architecture of the adaptive model generation system allows machine learning algorithms use data from multiple sources just as easily as data from one Source. This allows correlation algorithms to be integrated into the adaptive model generation framework which could potentially increase the performance of an intrusion detection system. Accordingly, multiple different types of data Sources, and alert streams, can be algorithmically combined to detect a wider range of attacks, or even coordinated attacks targeting multiple sites. In accordance with the invention, the object

Claim	Exemplary Citation from Honig
	described above have been met, and the need in the art for an effective intrusion detection architecture has been satisfied." Honig at 6:50: "The system in accordance with the present invention (also referred to as "Adaptive Model Generation' or AMG) is an architecture which provides and automates many of the critical processes in the deployment and operation of real time data mining-based intrusion detection systems. The system abstracts various parts of the data mining-based IDS process and formalizes the automation of this process. This includes abstracting the processes of data collection, data aggregation, detection model evaluation, detection model generation, and model distribution. The system uses a general XML-based data and model representation scheme that facilitates the translation of data from what is collected at the audit stream to the form necessary for generation of detection models." Honig at 7:8: "More specifically, the system has the following major capabilities: Automated data collection is provided, in which data is collected by sensors and automatically sent to detectors for classification and to the data warehouse for aggregation and use in training models. Data warehousing capabilities is provided by a data warehouse component that stores data from all sensors. This data is used for training detection models, but also may be used to Support various types of data analysis Such as forensic analysis. Automated model generation trains detection models from data stored in the data warehouse. The process for converting the data into the appropriate form for training is fully automated. Heterogeneous data Support permits the handling of data from different types of audit sources. This capability is allowed since any form of data can be represented using a general XML-based language." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the

Claim	Exemplary Citation from Honig
	data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 12:17: "The data warehouse 14 is described herein. It serves as the central storage repository for all of the data collected by the sensors 12. The model generators 16 access the data in the data warehouse 14 and create detection models using this data. The data warehouse 14 also stores these detection models. The analysis engines 22, 24, 26, and 28 also access the data stored in the data warehouse 14." Honig at 12:35: "For example, if there are 40 Windows™ hosts in a network, in order to create an anomaly detection model over the application Event logs for each of the hosts in the system framework, the following steps must be performed. A sensor 12 is installed on each of the hosts. This sensor collects the data and stores it in the data warehouse 14. If each host is typically used in the same way, a large data set may be created containing the combined event logs from each of the hosts." Honig at 14:5: "The model generation modules 16 request the data from the data warehouse 14 when they want to create a model. They form their request based on the information that the model needs to train on. The generator 16 then runs and creates a model. This model is then encoded into XML and sent to the data warehouse 14. Model generators 16 also signal the model distributor 18 to let it know that a new model is available. A sample XML encoding of a model generated by the RAD system is shown

	below." Honig at 21:13: "The adaptive model generation framework Supports the creation of anomaly detection models. Since sensors send data to the data warehouse, it is easy to aggregate the data for collection. Using the forensics analysis engine, it is possible to see if the data is clean and contains no intrusions. This can greatly decrease the cost of creating the training set since it speeds the process of Verifying that the data is clean. The model generators can automatically generate anomaly detection models using the data from the data warehouse and deploy the detection models using the model distributor. Unsupervised anomaly detection algorithms examine unlabeled data and attempt to detect intrusions buried within the unlabeled data. Unsupervised anomaly detection algorithms operate under the principle that intrusions are very rare compared to the normal data and they are also quantitatively different. Because of this, intrusions are outliers in the data and can be detected. Since unsupervised anomaly detection can detect intrusions in an unlabeled data set, they are used inside the forensics analysis engines. Data from the data warehouse is sent to a forensics analysis engine where an unsupervised anomaly detection algorithm is applied. The forensics analysis engine can label the data which it determines to be an outlier. Unsupervised anomaly detection algorithms can also be used to help label data that is collected by the system. This labeled data can then be used to train a misuse or anomaly detection model." Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20."
--	---

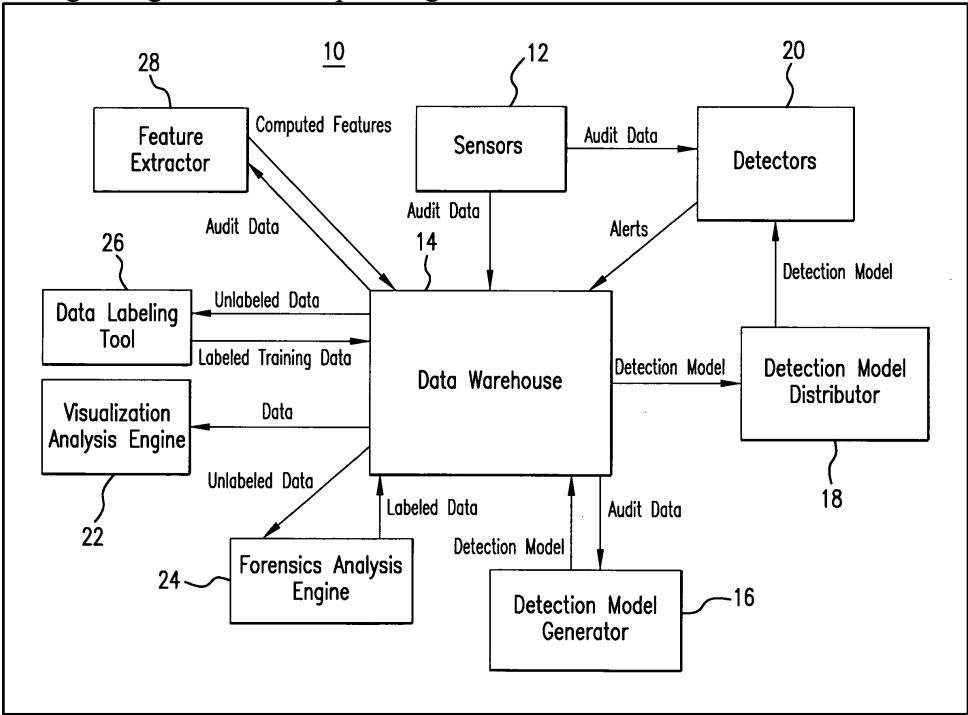
Claim	Exemplary Citation from Honig
	Honig at 26:11: "The multiplicity of this system can easily be increased with the novel system described herein. With no changes in architecture, the system can Support any number of host machines and sensors. With a conventional system architecture, increasing the multiplicity would require major changes in the structure of a system. According to the invention, the central data collection is automated in the system. This means that data from multiple machines is gathered in the same place and can be analyzed from that central location." Honig at Fig. 1 and corresponding text:  <pre> graph TD 12[Sensors] -- Audit Data --> 14[Data Warehouse] 14 -- Audit Data --> 28[Feature Extractor] 14 -- Audit Data --> 20[Detectors] 28 -- Computed Features --> 14 26[Data Labeling Tool] -- Unlabeled Data --> 14 14 -- Labeled Training Data --> 26 14 -- Data --> 22[Visualization Analysis Engine] 24[Forensics Analysis Engine] -- Labeled Data --> 14 14 -- Unlabeled Data --> 24 16[Detection Model Generator] -- Detection Model --> 14 14 -- Audit Data --> 16 14 -- Detection Model --> 18[Detection Model Distributor] 18 -- Detection Model --> 20 20 -- Alerts --> 14 </pre> See also Honig at 11:8-61, 20:39-27:57.
[9] The method of claim 1, wherein the adaptive	Honig discloses and/or renders obvious that the adaptive reference model is generated to include a value layer that determines whether an asset value contained in a snapshot is anomalous.

Claim	Exemplary Citation from Honig
reference model is generated to include a value layer that determines whether an asset value contained in a snapshot is anomalous.	Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 5:61: "A system for detecting intrusions in the operation of a computer system is disclosed herein which comprises a plurality of sensors configured to gather information regarding the operation of the computer system, to format the information into data records having a predetermined format, and to transmit the data in the predetermined data format. A plurality of detection model generators may be configured to request data records from the data warehouse in the predetermined data format. Each detection model generator is configured to generate a respective intrusion detection model based on said data records, and to transmit the respective intrusion detection model to the data warehouse according to the predetermined data format. The invention provides a number of advantages, including the Support of heterogeneous data, a central storage of data at the data warehouse, and a common data format enables the system to combine data from different sources very easily. The distributed architecture of the adaptive model generation system allows machine learning algorithms use data from multiple sources just as easily as data from one Source. This allows correlation algorithms to be integrated into the adaptive model generation framework which could potentially increase the performance of an intrusion detection system. Accordingly, multiple different types of data Sources, and alert streams, can be algorithmically combined to detect a wider range of attacks, or even coordinated attacks targeting multiple sites. In accordance with the invention, the object

Claim	Exemplary Citation from Honig
	described above have been met, and the need in the art for an effective intrusion detection architecture has been satisfied." Honig at 6:50: "The system in accordance with the present invention (also referred to as "Adaptive Model Generation' or AMG) is an architecture which provides and automates many of the critical processes in the deployment and operation of real time data mining-based intrusion detection systems. The system abstracts various parts of the data mining-based IDS process and formalizes the automation of this process. This includes abstracting the processes of data collection, data aggregation, detection model evaluation, detection model generation, and model distribution. The system uses a general XML-based data and model representation scheme that facilitates the translation of data from what is collected at the audit stream to the form necessary for generation of detection models." Honig at 7:8: "More specifically, the system has the following major capabilities: Automated data collection is provided, in which data is collected by sensors and automatically sent to detectors for classification and to the data warehouse for aggregation and use in training models. Data warehousing capabilities is provided by a data warehouse component that stores data from all sensors. This data is used for training detection models, but also may be used to Support various types of data analysis Such as forensic analysis. Automated model generation trains detection models from data stored in the data warehouse. The process for converting the data into the appropriate form for training is fully automated. Heterogeneous data Support permits the handling of data from different types of audit sources. This capability is allowed since any form of data can be represented using a general XML-based language." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the

Claim	Exemplary Citation from Honig
	data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 12:17: "The data warehouse 14 is described herein. It serves as the central storage repository for all of the data collected by the sensors 12. The model generators 16 access the data in the data warehouse 14 and create detection models using this data. The data warehouse 14 also stores these detection models. The analysis engines 22, 24, 26, and 28 also access the data stored in the data warehouse 14." Honig at 12:35: "For example, if there are 40 Windows™ hosts in a network, in order to create an anomaly detection model over the application Event logs for each of the hosts in the system framework, the following steps must be performed. A sensor 12 is installed on each of the hosts. This sensor collects the data and stores it in the data warehouse 14. If each host is typically used in the same way, a large data set may be created containing the combined event logs from each of the hosts." Honig at 14:5: "The model generation modules 16 request the data from the data warehouse 14 when they want to create a model. They form their request based on the information that the model needs to train on. The generator 16 then runs and creates a model. This model is then encoded into XML and sent to the data warehouse 14. Model generators 16 also signal the model distributor 18 to let it know that a new model is available. A sample XML encoding of a model generated by the RAD system is shown

Claim	Exemplary Citation from Honig
	below." Honig at 21:13: "The adaptive model generation framework Supports the creation of anomaly detection models. Since sensors send data to the data warehouse, it is easy to aggregate the data for collection. Using the forensics analysis engine, it is possible to see if the data is clean and contains no intrusions. This can greatly decrease the cost of creating the training set since it speeds the process of Verifying that the data is clean. The model generators can automatically generate anomaly detection models using the data from the data warehouse and deploy the detection models using the model distributor. Unsupervised anomaly detection algorithms examine unlabeled data and attempt to detect intrusions buried within the unlabeled data. Unsupervised anomaly detection algorithms operate under the principle that intrusions are very rare compared to the normal data and they are also quantitatively different. Because of this, intrusions are outliers in the data and can be detected. Since unsupervised anomaly detection can detect intrusions in an unlabeled data set, they are used inside the forensics analysis engines. Data from the data warehouse is sent to a forensics analysis engine where an unsupervised anomaly detection algorithm is applied. The forensics analysis engine can label the data which it determines to be an outlier. Unsupervised anomaly detection algorithms can also be used to help label data that is collected by the system. This labeled data can then be used to train a misuse or anomaly detection model." Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20."

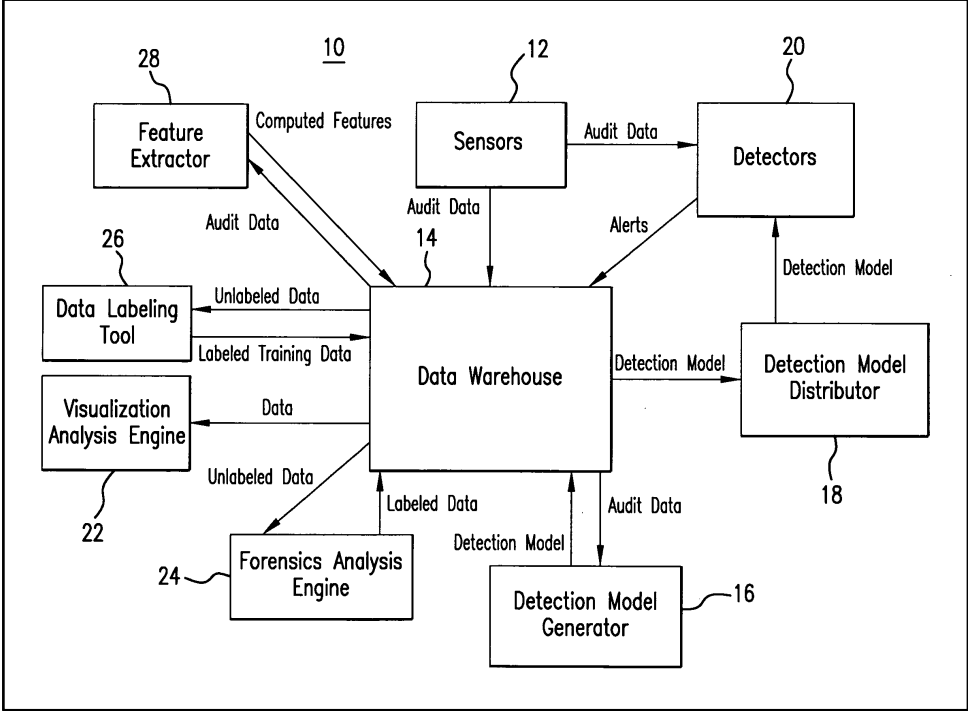
Claim	Exemplary Citation from Honig
	Honig at 26:11: "The multiplicity of this system can easily be increased with the novel system described herein. With no changes in architecture, the system can Support any number of host machines and sensors. With a conventional system architecture, increasing the multiplicity would require major changes in the structure of a system. According to the invention, the central data collection is automated in the system. This means that data from multiple machines is gathered in the same place and can be analyzed from that central location." Honig at Fig. 1 and corresponding text:  See also Honig at 11:8-61, 20:39-27:57.
[10] The method of claim 1, wherein the adaptive reference model is	Honig discloses and/or renders obvious that the adaptive reference model is generated to include a cluster layer that tracks relationships between assets and identifies an anomaly in response to an asset being unexpectedly absent from or present in a set of assets in a snapshot.

Claim	Exemplary Citation from Honig
generated to include a cluster layer that tracks relationships between assets and identifies an anomaly in response to an asset being unexpectedly absent from or present in a set of assets in a snapshot.	Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 5:61: "A system for detecting intrusions in the operation of a computer system is disclosed herein which comprises a plurality of sensors configured to gather information regarding the operation of the computer system, to format the information into data records having a predetermined format, and to transmit the data in the predetermined data format. A plurality of detection model generators may be configured to request data records from the data warehouse in the predetermined data format. Each detection model generator is configured to generate a respective intrusion detection model based on said data records, and to transmit the respective intrusion detection model to the data warehouse according to the predetermined data format. The invention provides a number of advantages, including the Support of heterogeneous data, a central storage of data at the data warehouse, and a common data format enables the system to combine data from different sources very easily. The distributed architecture of the adaptive model generation system allows machine learning algorithms use data from multiple sources just as easily as data from one Source. This allows correlation algorithms to be integrated into the adaptive model generation framework which could potentially increase the performance of an intrusion detection system. Accordingly, multiple different types of data Sources, and alert streams, can be algorithmically combined to detect a wider range of attacks, or even coordinated attacks targeting multiple sites. In accordance with the invention, the object

Claim	Exemplary Citation from Honig
	described above have been met, and the need in the art for an effective intrusion detection architecture has been satisfied." Honig at 6:50: "The system in accordance with the present invention (also referred to as "Adaptive Model Generation' or AMG) is an architecture which provides and automates many of the critical processes in the deployment and operation of real time data mining-based intrusion detection systems. The system abstracts various parts of the data mining-based IDS process and formalizes the automation of this process. This includes abstracting the processes of data collection, data aggregation, detection model evaluation, detection model generation, and model distribution. The system uses a general XML-based data and model representation scheme that facilitates the translation of data from what is collected at the audit stream to the form necessary for generation of detection models." Honig at 7:8: "More specifically, the system has the following major capabilities: Automated data collection is provided, in which data is collected by sensors and automatically sent to detectors for classification and to the data warehouse for aggregation and use in training models. Data warehousing capabilities is provided by a data warehouse component that stores data from all sensors. This data is used for training detection models, but also may be used to Support various types of data analysis Such as forensic analysis. Automated model generation trains detection models from data stored in the data warehouse. The process for converting the data into the appropriate form for training is fully automated. Heterogeneous data Support permits the handling of data from different types of audit sources. This capability is allowed since any form of data can be represented using a general XML-based language." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the

Claim	Exemplary Citation from Honig
	data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 12:17: "The data warehouse 14 is described herein. It serves as the central storage repository for all of the data collected by the sensors 12. The model generators 16 access the data in the data warehouse 14 and create detection models using this data. The data warehouse 14 also stores these detection models. The analysis engines 22, 24, 26, and 28 also access the data stored in the data warehouse 14." Honig at 12:35: "For example, if there are 40 Windows™ hosts in a network, in order to create an anomaly detection model over the application Event logs for each of the hosts in the system framework, the following steps must be performed. A sensor 12 is installed on each of the hosts. This sensor collects the data and stores it in the data warehouse 14. If each host is typically used in the same way, a large data set may be created containing the combined event logs from each of the hosts." Honig at 14:5: "The model generation modules 16 request the data from the data warehouse 14 when they want to create a model. They form their request based on the information that the model needs to train on. The generator 16 then runs and creates a model. This model is then encoded into XML and sent to the data warehouse 14. Model generators 16 also signal the model distributor 18 to let it know that a new model is available. A sample XML encoding of a model generated by the RAD system is shown

Claim	Exemplary Citation from Honig
	below." Honig at 21:13: "The adaptive model generation framework Supports the creation of anomaly detection models. Since sensors send data to the data warehouse, it is easy to aggregate the data for collection. Using the forensics analysis engine, it is possible to see if the data is clean and contains no intrusions. This can greatly decrease the cost of creating the training set since it speeds the process of Verifying that the data is clean. The model generators can automatically generate anomaly detection models using the data from the data warehouse and deploy the detection models using the model distributor. Unsupervised anomaly detection algorithms examine unlabeled data and attempt to detect intrusions buried within the unlabeled data. Unsupervised anomaly detection algorithms operate under the principle that intrusions are very rare compared to the normal data and they are also quantitatively different. Because of this, intrusions are outliers in the data and can be detected. Since unsupervised anomaly detection can detect intrusions in an unlabeled data set, they are used inside the forensics analysis engines. Data from the data warehouse is sent to a forensics analysis engine where an unsupervised anomaly detection algorithm is applied. The forensics analysis engine can label the data which it determines to be an outlier. Unsupervised anomaly detection algorithms can also be used to help label data that is collected by the system. This labeled data can then be used to train a misuse or anomaly detection model." Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20."

Claim	Exemplary Citation from Honig
	Honig at 26:11: "The multiplicity of this system can easily be increased with the novel system described herein. With no changes in architecture, the system can Support any number of host machines and sensors. With a conventional system architecture, increasing the multiplicity would require major changes in the structure of a system. According to the invention, the central data collection is automated in the system. This means that data from multiple machines is gathered in the same place and can be analyzed from that central location." Honig at Fig. 1 and corresponding text:  <pre> graph TD 10[10] --- 12[Sensors 12] 10 --- 20[Detectors 20] 10 --- 26[Data Labeling Tool 26] 10 --- 22[Visualization Analysis Engine 22] 10 --- 24[Forensics Analysis Engine 24] 10 --- 16[Detection Model Generator 16] 10 --- 18[Detection Model Distributor 18] 10 --- 28[Feature Extractor 28] 10 --- 14[Data Warehouse 14] 12 -- "Audit Data" --> 14 20 -- "Alerts" --> 14 26 -- "Unlabeled Data" --> 14 14 -- "Labeled Training Data" --> 26 22 -- "Data" --> 22 24 -- "Unlabeled Data" --> 14 14 -- "Labeled Data" --> 24 16 -- "Audit Data" --> 14 14 -- "Detection Model" --> 16 14 -- "Detection Model" --> 18 18 -- "Detection Model" --> 20 28 -- "Computed Features" --> 14 14 -- "Audit Data" --> 28 </pre> See also Honig at 11:8-61, 20:39-27:57.

Claim	Exemplary Citation from Honig
[11] The method of claim 1, wherein the adaptive reference model is generated to include a profile layer that identifies anomalies in response to violation of relationships of clusters of assets in a snapshot.	Honig discloses and/or renders obvious that the adaptive reference model is generated to include a profile layer that identifies anomalies in response to violation of relationships of clusters of assets in a snapshot. Honig at Abstract: "A system and methods for detecting intrusions in the operation of a computer system comprises a sensor configured to gather information regarding the operation of the computer system, to format the information in a data record having a predetermined format, and to transmit the data in the predetermined data format. A data warehouse is configured to receive the data record from the sensor in the predetermined data format and to store the data in a database. A detection model generator is configured to request data records from the data warehouse in the predetermined data format, to generate an intrusion detection model based on said data records, and to transmit the intrusion detection model to the data warehouse according to the predetermined data format. A detector is configured to receive a data record in the predetermined data format from the sensor and to classify the data record in real-time as one of normal operation and an attack based on said intrusion detection model. A data analysis engine is configured to request data records from the data warehouse according to the predetermined data format and to perform a data processing function on the data records." Honig at 5:61: "A system for detecting intrusions in the operation of a computer system is disclosed herein which comprises a plurality of sensors configured to gather information regarding the operation of the computer system, to format the information into data records having a predetermined format, and to transmit the data in the predetermined data format. A plurality of detection model generators may be configured to request data records from the data warehouse in the predetermined data format. Each detection model generator is configured to generate a respective intrusion detection model based on said data records, and to transmit the respective intrusion detection model to the data warehouse according to the predetermined data format. The invention provides a number of advantages, including the Support of heterogeneous data, a central storage of data at the data warehouse, and a common data format enables the system to combine data from different sources very easily. The distributed architecture of the adaptive model generation system allows machine learning algorithms use data from multiple sources just as easily as data from one Source. This allows correlation

Claim	Exemplary Citation from Honig
	algorithms to be integrated into the adaptive model generation framework which could potentially increase the performance of an intrusion detection system. Accordingly, multiple different types of data Sources, and alert streams, can be algorithmically combined to detect a wider range of attacks, or even coordinated attacks targeting multiple sites. In accordance with the invention, the object described above have been met, and the need in the art for an effective intrusion detection architecture has been satisfied." Honig at 6:50: "The system in accordance with the present invention (also referred to as "Adaptive Model Generation' or AMG) is an architecture which provides and automates many of the critical processes in the deployment and operation of real time data mining-based intrusion detection systems. The system abstracts various parts of the data mining-based IDS process and formalizes the automation of this process. This includes abstracting the processes of data collection, data aggregation, detection model evaluation, detection model generation, and model distribution. The system uses a general XML-based data and model representation scheme that facilitates the translation of data from what is collected at the audit stream to the form necessary for generation of detection models." Honig at 7:8: "More specifically, the system has the following major capabilities: Automated data collection is provided, in which data is collected by sensors and automatically sent to detectors for classification and to the data warehouse for aggregation and use in training models. Data warehousing capabilities is provided by a data warehouse component that stores data from all sensors. This data is used for training detection models, but also may be used to Support various types of data analysis Such as forensic analysis. Automated model generation trains detection models from data stored in the data warehouse. The process for converting the data into the appropriate form for training is fully automated. Heterogeneous data Support permits the handling of data from different types of audit sources. This capability is allowed since any form of data can be represented using a general XML-based language." Honig at 7:25: "Automated model distribution is provided. Once a new model is generated, it may be deployed to all of the detectors that subscribe to the particular detection models that have been generated. The

Claim	Exemplary Citation from Honig
	system enables evaluation of archival records stored within the data warehouse to search for intrusions. The system includes generic visualization components that allow in a consistent fashion the visualization of data from different sources. The system also provides correlation Support. Since data from multiple sensors is stored in the data warehouse, the system can perform analysis over the data from multiple sources and to train detection models which examine audit streams from multiple sensors. The system is designed to be extensible and Scalable, and hence any audit Source, any Supervised learning module, any unsupervised (anomaly detection) learning model may be easily inserted into the architecture. In addition, any correlation function or algorithm may be easily inserted to combine information from multiple sources to provide better coverage of attacks, be they coordinated distributed attacks, or clever new attacks against multiple targets within the protected LAN. Moreover, the architecture design also allows for scalability in large networks, and high bandwidth environments. The system architecture can easily be distributed to multiple processors to increase the speed of operation, and it can utilize a high capacity data warehouse (e.g., a parallel or distributed Relational Database Management System (RDBMS))." Honig at 12:17: "The data warehouse 14 is described herein. It serves as the central storage repository for all of the data collected by the sensors 12. The model generators 16 access the data in the data warehouse 14 and create detection models using this data. The data warehouse 14 also stores these detection models. The analysis engines 22, 24, 26, and 28 also access the data stored in the data warehouse 14." Honig at 12:35: "For example, if there are 40 Windows™ hosts in a network, in order to create an anomaly detection model over the application Event logs for each of the hosts in the system framework, the following steps must be performed. A sensor 12 is installed on each of the hosts. This sensor collects the data and stores it in the data warehouse 14. If each host is typically used in the same way, a large data set may be created containing the combined event logs from each of the hosts." Honig at 14:5: "The model generation modules 16 request the data from the data warehouse 14 when they want to create a model. They form their request based on the information that the model needs to train on.

Claim	Exemplary Citation from Honig
	The generator 16 then runs and creates a model. This model is then encoded into XML and sent to the data warehouse 14. Model generators 16 also signal the model distributor 18 to let it know that a new model is available. A sample XML encoding of a model generated by the RAD system is shown below." Honig at 21:13: "The adaptive model generation framework Supports the creation of anomaly detection models. Since sensors send data to the data warehouse, it is easy to aggregate the data for collection. Using the forensics analysis engine, it is possible to see if the data is clean and contains no intrusions. This can greatly decrease the cost of creating the training set since it speeds the process of Verifying that the data is clean. The model generators can automatically generate anomaly detection models using the data from the data warehouse and deploy the detection models using the model distributor. Unsupervised anomaly detection algorithms examine unlabeled data and attempt to detect intrusions buried within the unlabeled data. Unsupervised anomaly detection algorithms operate under the principle that intrusions are very rare compared to the normal data and they are also quantitatively different. Because of this, intrusions are outliers in the data and can be detected. Since unsupervised anomaly detection can detect intrusions in an unlabeled data set, they are used inside the forensics analysis engines. Data from the data warehouse is sent to a forensics analysis engine where an unsupervised anomaly detection algorithm is applied. The forensics analysis engine can label the data which it determines to be an outlier. Unsupervised anomaly detection algorithms can also be used to help label data that is collected by the system. This labeled data can then be used to train a misuse or anomaly detection model." Honig at 24:32: "Like the misuse detection algorithm, unsupervised anomaly detection requires training data. During a training period, a system is run normally with no attacks. Sensors 12 monitoring the system send their observations via XML to the data warehouse 14. Although no attacks are intentionally run, if some unknown attacks were to occur, there would be no problem. The algorithm can tolerate some noise (un known attacks) and still generalize well. Once enough training data has been accumulated it is sent from the data warehouse 14 to the model generator 16 via XML. There is no need to label data. The model generator 16 then uses the unsupervised SVM algorithm to generate a model of

Claim	Exemplary Citation from Honig
	normal activity. This model is made up of the set of support vectors and their associated weights. The model is then sent to the data warehouse 14 for storage and to the appropriate detectors 20." Honig at 26:11: "The multiplicity of this system can easily be increased with the novel system described herein. With no changes in architecture, the system can Support any number of host machines and sensors. With a conventional system architecture, increasing the multiplicity would require major changes in the structure of a system. According to the invention, the central data collection is automated in the system. This means that data from multiple machines is gathered in the same place and can be analyzed from that central location." Honig at Fig. 1 and corresponding text:

Claim	Exemplary Citation from Honig
	<i>See also</i> Honig at 11:8-61, 20:39-27:57.
[12PRE] A computer readable medium storing instructions, that when executed by a computer, cause the computer to perform functions of:	<i>See</i> [1PRE].
[12A] receiving snapshots from a plurality of computers within a population of computers, wherein individual snapshots include data indicating a state of a respective computer;	<i>See</i> [1A].
[12B] automatically generating an adaptive reference model comprising a rule set customized to characteristics of the population of computers, the rule set being developed by identifying patterns among the snapshots from the plurality of computers such that the adaptive reference model is indicative of normal states in the computers within the population; and	<i>See</i> [1B].
[12C] comparing a snapshot from at least one of the	<i>See</i> [1C].

Claim	Exemplary Citation from Honig
computers to the adaptive reference model to determine whether an anomaly is present in the state of the at least one of the computers.	
[13] The computer readable medium of claim 12, further comprising instructions, that when executed, cause the computer to compare the anomaly to a recognition filter to diagnose a trouble condition on the at least one of the computers, and, in the event of a trouble condition, to generate an automated response to the trouble condition.	<i>See Claim 2.</i>
[14PRE] The computer readable medium of claim 13, wherein the automated response is a generic response not specific to a particular asset of the at least one computer, and wherein the computer readable medium further comprises instructions, that when executed, cause the computer to:	<i>See [3PRE].</i>

Claim	Exemplary Citation from Honig
[14A] send the generic response and a set of anomalies found in the snapshot to the at least one computer, the set of anomalies indicating assets of the at least one computer whose states are anomalous; and	<i>See</i> [3A].
[14B] apply the generic response to the anomalous assets to correct the trouble condition.	<i>See</i> [3B].
[15] The computer readable medium of claim 14, wherein the generic responses include at least one of: installing a missing software component, removing an undesirable software component, and restoring an incorrect registry setting.	<i>See</i> Claim 4.
[16] The computer readable medium of claim 13, wherein the recognition filter comprises a particular pattern of anomalies that indicates the presence of a particular root cause condition or a generic class of conditions.	<i>See</i> Claim 5.

Claim	Exemplary Citation from Honig
[17] The computer readable medium of claim 12, wherein the instructions for comparing the snapshot to the adaptive reference model include instructions for determining whether an asset value contained in a snapshot is anomalous.	<i>See Claim 9.</i>
[18] The computer readable medium of claim 12, wherein the instructions for comparing the snapshot to the adaptive reference model include instructions for tracking relationships between assets and identifying an anomaly in response to an asset being unexpectedly absent from or present in a set of assets in a snapshot.	<i>See Claim 10.</i>
[19] The computer readable medium of claim 12, wherein the instructions for comparing the snapshot to the adaptive reference model include instructions for identifying anomalies in response to violation of relationships of clusters of assets in a snapshot.	<i>See Claim 11.</i>

Claim	Exemplary Citation from Honig
[20PRE] The computer readable medium of claim 12, wherein the computer readable medium further comprises instructions, that when executed, cause the computer to:	<i>See</i> [6PRE].
[20A] compare a plurality of anomalies associated with a particular snapshot with a recognition filter to diagnose a trouble condition; and	<i>See</i> [6A].
[20B] diagnose a trouble condition on the at least one of the computers in response to at least a subset of the plurality of anomalies matching information in the recognition filter.	<i>See</i> [6B].
[21] The computer readable medium of claim 12, wherein individual snapshots include data associated with at least one of: system files, application files, a registry entry, a performance counter, a process, a communication port, a hardware configuration, a log file, a	<i>See</i> Claim 7.

Claim	Exemplary Citation from Honig
running task, services, and network connections.	
[22] The computer readable medium of claim 12, wherein the computer readable medium further comprises instructions, that when executed, cause the computer to: insert rules into the rule set of the adaptive reference model to augment or override rules of the rule set automatically generated from the snapshots.	See Claim 8.