SERVICENOW

EXHIBIT A	
Quantar's Preliminary Infringement Contentions	
US Patent No: 9143523 12/811,208	**Accused Instrumentalities**
Claim: 1	
1. Apparatus for assessing threat to at least one computer network, the threat including at least one electronic threat, the computer network comprising a plurality of IT systems and a plurality of business processes operating on the plurality of IT systems, wherein (a) at least one IT system has two or more of the plurality of business processes operating thereon or (b) at least one business process operates on two or more of the plurality of IT systems, the apparatus comprising at least one processor and a memory coupled to the processor, the memory storing instructions executable by the processor that cause the processor to:	
predict future threat activity based on past observed threat activity including, for the at least one electronic threat, to receive observed threat data from a database, to extrapolate future event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target,	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

determine expected downtime of each system of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency, determine loss for each of the plurality of business processes dependent on the downtimes of the IT systems, and add losses for the plurality of business processes so as to obtain a combined loss arising from the threat activity.	
Claim: 12	
12. A method of assessing threat to at least one computer network, the threat including at least one electronic threat, the network comprising a plurality of IT systems wherein a plurality of business processes operate on the plurality of IT systems, and wherein (a) at least one IT system has two or more of the plurality of business processes operating thereon or (b) at least one business process operates on two or more of the plurality of IT systems, the method comprising, by using at least one computer processor:	
predicting threat activity based on past observed activity including, for the at least one electronic threat, to receive observed threat data from a database, to extrapolate future event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

determining expected downtime of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determining loss for the plurality of business processes dependent on the downtimes of the IT systems;	
adding losses for the plurality of business processes to obtain a combined loss arising from the threat activity.	
Claim: 15	
15. A non-transitory computer readable medium storing a computer program which when executed by a computer system, causes the computer system to perform a method of assessing threat to at least one computer network, the threat including at least one electronic threat, the computer network comprising a plurality of IT systems wherein a plurality of business processes operate on the plurality of IT systems, and wherein (a) at least one IT system has two or more of the plurality of business processes operating thereon or (b) at least one business process operates on two or more of the plurality of IT systems, the method comprising:	

predicting threat activity based on past observed activity including, for the at least one electronic threat, to receive observed threat data from a database, to extrapolate future event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determining expected downtime of each of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency;	
determining loss for the plurality of business processes dependent on the downtimes of the IT systems;	
adding losses for the plurality of business processes to obtain a combined loss arising from the threat activity.	

Note: Total claims: 15 and Independent claims: 3

EXHIBIT B	
Quantar's Preliminary Infringement Contentions	
US Patent No: 9363279 13/322,298	**Accused Instrumentalities**
Claim: 1	

1. An apparatus including one or more computer processors and a non-transient computer readable memory, wherein the one or more computer processors are configured pursuant to programming code in a the non-transient computer readable memory to predict, for each of a plurality of threats capable of affecting at least one computer network in which a plurality of systems operate, future threat activity using a Monte Carlo method based on stochastic modelling of past observed threat events, wherein the plurality of threats includes a plurality of electronic threats and the plurality of electronic threats includes a plurality of computer viruses, wherein the one or more computer processors are configured, for a given threat, to model a set of past observed threat events to obtain an estimate of at least one model parameter, and, in a Monte Carlo simulation of a given threat, to predict future threat events using the at least one model parameter and a stochastic model using a projection of at least one model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable, and to predict a distribution of future threat events by repeating the simulation using a plurality of variables; and	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
wherein the apparatus is further configured to determine an expected downtime of each of said systems in dependence upon said predicted future threat activity and to determine a financial loss for each of a plurality of operational processes dependent on the	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT

downtimes of each of said systems and to add the financial losses for said plurality of processes so as to obtain a combined financial loss arising from the predicted future threat activity.	Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise **SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
Claim: 25	
25. A computer-implemented method, the method being performed by a computer system having one or more computer processors and a non-transient computer readable memory, the one or more computer processors being configured pursuant to programming code in the non-transient computer readable memory, the method comprising:	
predicting, for each of a plurality of threats, future threat activity using a Monte Carlo method based on stochastic modelling of past observed threat events capable of affecting at least one computer network in which a plurality of systems operate, wherein the plurality of threats includes a plurality of electronic	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

threats and the plurality of electronic threats includes a plurality of computer viruses;	
wherein for each given threat the method comprises:	
modelling a set of past observed threat events to obtain an estimate of at least one model parameter;	
performing a Monte Carlo simulation of the given threat by:	
predicting future threat events using the at least one model parameter and a stochastic model using a projection of at least one model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable, and predicting a distribution of future threat events by repeating the simulation using a plurality of variables; and	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
wherein determining an expected downtime of each system in dependence upon said predicted future threat activity;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

determining a financial loss for each of a plurality of operational processes dependent on the downtimes of the systems;	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
adding the financial losses for the plurality of processes to obtain a combined financial loss arising from the future threat activity.	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
Claim: 29	
29. A non-transitory computer readable medium having a computer program thereon, which when executed by a computer system having one or more computer processors and a non-transient computer readable memory, causes the computer system to	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT

predict, for each of a plurality of threats, future threat activity a Monte Carlo method based on stochastic modelling of past observed threat events capable of affecting at least one computer network in which a plurality of systems operate, wherein the plurality of threats includes a plurality of electronic threats and the plurality of electronic threats includes a plurality of computer viruses;	Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
wherein execution of the computer program causes the computer system to perform, for each given threat, steps comprising:	
modelling a set of past observed threat events to obtain an estimate of at least one model parameter;	
performing a Monte Carlo simulation of the given threat by:	
predicting future threat events using the at least one model parameter and a stochastic model using a projection of at least one model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable, and predicting a distribution of future threat events by repeating the simulation using a plurality of variables; and	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

wherein determining an expected downtime of each system in dependence upon said predicted future threat activity;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determining a financial loss for each of a plurality of operational processes dependent on the downtimes of the systems;	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
adding the financial losses for the plurality of processes to obtain a combined financial loss arising from the future threat activity.	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.

Note: Total claims: 30 and Independent claims: 3

EXHIBIT C	
Quantar's Preliminary Infringement Contentions	
US Patent No: 9288224 14/827,712	**Accused Instrumentalities**
Claim: 1	
1. Apparatus for assessing and valuing computer network threats, the threats including at least one electronic threat, the computer network comprising a plurality of IT systems and a plurality of business processes operating on the plurality of IT systems, the apparatus comprising at least one processor and a memory coupled to the processor, the memory storing instructions executable by the processor that cause the processor to:	
predict future threat activity based on past observed threat activity including, at least one electronic threat, to receive observed threat data from a database, to extrapolate future event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

determine expected downtime of each system of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determine the financial loss for each of the plurality of business processes dependent on the downtimes of the IT systems, and;	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
add the financial losses for the plurality of business processes so as to obtain a combined financial loss arising from the threat activity.	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary

	terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
Claim: 13	
13. A method of assessing and valuing computer network threats, the threats including at least one electronic threat, the network comprising a plurality of IT systems wherein a plurality of business processes operate on the plurality of IT systems the method comprising, by using at least one computer processor:	
predicting threat activity based on past observed activity including, for at least one electronic threat, to receive observed threat data from a database, to extrapolate future event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determining expected downtime of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of

	an event based on data aggregated across your extended enterprise
determining the financial loss for the plurality of business processes dependent on the downtimes of the IT systems;	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
adding the financial losses for the plurality of business processes to obtain a combined financial loss arising from the threat activity.	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
Claim: 16	
16. A non-transitory computer readable medium storing a computer program which when executed by a	

computer system, causes the computer system to perform a method of assessing and valuing computer network threats, the threats including at least one electronic threat, the computer network comprising a plurality of IT systems wherein a plurality of business processes operate on the plurality of IT systems, the method comprising:	
predicting threat activity based on past observed activity including, at least one electronic threat, to receive observed threat data from a database, to extrapolate future event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determining expected downtime of each of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

determining the financial loss for the plurality of business processes dependent on the downtimes of the IT systems;	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
adding the financial losses for the plurality of business processes to obtain a combined financial loss arising from the threat activity.	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.

Note: Total claims: 16 and Independent claims: 3

EXHIBIT D	
Quantar's Preliminary Infringement Contentions	
US Patent No: 9418226 15/017,645	**Accused Instrumentalities**
Claim: 1	
1. Apparatus for assessing financial loss from threats capable of affecting at least one computer network, a network includes a plurality of interconnected networks, the threats including at least one electronic threat, the computer network comprising a plurality of IT systems, an IT system defined in terms of physical location, and a plurality of operational business processes operating on the plurality of IT systems, the apparatus including one or more computer processors and a computer readable memory in which programming code is stored, wherein the one or more computer processors are configured pursuant to programming code in the computer readable memory to, predict for each of a plurality of threats capable of affecting at least one computer network in which a plurality of systems operate, future threat activity based on past observed threat activity wherein the plurality of threats includes a plurality of electronic threats and the plurality of electronic threats includes a plurality of computer viruses, Trojan horses, computer worms, hacking and denial of service attacks, to receive observed threat data from a database, to extrapolate future threat event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise **SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.

more targets for the observed threat and a severity score for each target;	
determine expected downtime of each system of the plurality of IT systems independence upon said predicted threat activity including the severity scores and extrapolated future event frequency;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determine financial loss for each of the plurality of operational business processes dependent on the downtimes of the IT systems;	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
add financial losses for the plurality of business processes to obtain a combined financial loss arising from the threat activity.	**SERVICENOW 2** RiskLens Integration

	The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
Claim: 13	
13. A method for assessing financial loss from threats capable of affecting at least one computer network, a network includes a plurality of interconnected networks, the threats including at least one electronic threat, the computer network comprising a plurality of IT systems, an IT system defined in terms of physical location, and a plurality of operational business processes operating on the plurality of IT systems, the apparatus including one or more computer processors and a computer readable memory in which programming code is stored, wherein the one or more computer processors are configured pursuant to programming code in the computer readable memory to, predict for each of a plurality of threats capable of affecting at least one computer network in which a plurality of systems operate, future threat activity based on past observed threat activity wherein the plurality of threats includes a plurality of electronic threats and the plurality of electronic threats includes a plurality of computer viruses, Trojan horses, computer worms, hacking and denial of service attacks, to receive observed threat data from a database, to extrapolate future threat event	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise **SERVICENOW 2** <u>RiskLens Integration</u> The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.

frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target;	
determine expected downtime of each system of the plurality of IT systems independence upon said predicted threat activity including the severity scores and extrapolated future event frequency;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determine financial loss for each of the plurality of operational business processes dependent on the downtimes of the IT systems;	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.

add financial losses for the plurality of business processes to obtain a combined financial loss arising from the threat activity.	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
Claim: 16	
16. A non-transitory computer readable memory storing a computer program which when executed by a computer system, causes the computer system to perform a method of assessing financial loss from threats capable of affecting at least one computer network, a network include a plurality of interconnected networks, the threats including at least one electronic threat, the computer network comprising a plurality of IT systems, an IT system defined in terms of physical location, and a plurality of operational business processes operating on the plurality of IT systems, the method comprising:	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise **SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.

predict for each of a plurality of threats capable of affecting at least one computer network in which a plurality of systems operate, future threat activity based on past observed threat activity wherein the plurality of threats includes a plurality of electronic threats and the plurality of electronic threats includes a plurality of computer viruses, Trojan horses, computer worms, hacking and denial of service attacks, to receive observed threat data from a database, to extrapolate future threat event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determine expected downtime of each system of the plurality of IT systems independence upon said predicted threat activity including the severity scores and extrapolated future event frequency;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determine financial loss for each of the plurality of operational business processes dependent on the downtimes of the IT systems;	**SERVICENOW 2** RiskLens Integration

	The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
add financial losses for the plurality of business processes to obtain a combined financial loss arising from the threat activity.	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.

Note: Total claims: 16 and Independent claims: 3

EXHIBIT E	
Quantar's Preliminary Infringement Contentions	
US Patent No: 9762605 15/012,182	**Accused Instrumentalities**
Claim: 1	

1. Apparatus for assessing financial loss from cyber threats capable of affecting at least one computer network, the threat including at least one electronic threat, the computer network comprising a plurality of IT systems and a plurality of business processes operating on the plurality of IT systems, the apparatus comprising at least one processor configured pursuant to programming code in a non-transitory computer readable memory coupled to the processor, the non-transitory computer memory storing instructions executable by the processor that cause the processor to:	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
predict future cyber threat activity using a Monte Carlo method based on stochastic modeling of actual past observed computer network cyber threat activity, to receive observed cyber threat data from a database, the list of observed cyber threats including information, for each threat, of identification of at least one computer system targeted, to extrapolate future event frequency, to produce a profile of predicted cyber threat activity, wherein for each actual observed cyber threat on the computer network, an identifier, a name, a description of the threat, a temporal profile specifying frequency of occurrence, a target (or targets) for the threat and a severity score for the (each target) are included in the cyber threat data within the database, output the predicted future threat activity to one or more firewalls to improve their accuracy in correctly identifying cyber threats actually observed on the one or more computer networks to improve the accuracy of the apparatus and	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise **SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.

stochastic modeling of assessing financial loss from cyber threats on an ongoing basis, determine expected downtime of each system of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency, determine loss for each of the plurality of business processes dependent on the downtimes of the IT systems, and add losses for the plurality of business processes so as to obtain a combined financial loss arising from the cyber threat activity.	
Claim: 11	
11. A computer-implemented method, the method being performed by a computer system having one or more computer processors and a non-transitory computer readable memory in which programming code is stored, whereupon execution of the programming code by one or more computer processors the computer system performs operations comprising:	
predicting future cyber threat activity, for each of a plurality of computer network cyber threats, using a Monte Carlo method based on stochastic modeling of actual past observed computer network cyber threat activity, to receive observed cyber threat data from a database, the list of observed cyber threats including information, for each threat, of identification of at least one computer system targeted, to extrapolate future event frequency, to produce a profile of predicted cyber threat activity, wherein for each actual observed cyber	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise **SERVICENOW 2**

threat on the computer network, an identifier, a name, a description of the threat, a temporal profile specifying frequency of occurrence, a target (or targets) for the threat and a severity score for the (each target) are included in the cyber threat data within the database, output the predicted future threat activity to one or more firewalls to improve their accuracy in correctly identifying cyber threats actually observed on the one or more computer networks to improve the accuracy of the apparatus and stochastic modeling of assessing financial loss from cyber threats on an ongoing basis, wherein for each given threat the method comprises;	RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
modeling a set of past observed computer network cyber threat events to obtain an estimate of at least one model parameter;	
performing a Monte Carlo simulation of the given computer network cyber threat by:	
predicting future computer network cyber threat events using the at least one model parameter and a stochastic model using a projection of at least one model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable according to a predefined distribution and to use said at least one variable in the stochastic model and predicting a distribution of future computer network cyber threat events by repeating the simulation using a plurality of variables, determining expected downtime of each IT system in dependence upon said predicted future	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise **SERVICENOW 2**

computer network cyber threat activity, determining financial loss for each of a plurality of operational processes dependent on the downtimes of the IT systems adding losses for the plurality of processes to obtain a combined financial loss arising from the future computer network cyber threat activity.	RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
Claim: 13	
13. A computer readable medium having a computer program thereon, which when executed by a computer system having one or more computer processors and a non-transitory computer readable memory, causes the computer system to perform steps comprising:	
to predict, for each of a plurality of computer network cyber threats, future cyber threat activity using a Monte Carlo method based on stochastic modeling of actual past observed computer network cyber threat activity, to receive observed cyber threat data from a database, the list of observed cyber threats including information, for each threat, of identification of at least one computer system targeted, to extrapolate future event frequency, to produce a profile of predicted cyber threat activity, wherein for each actual observed cyber threat on the computer network, an identifier, a name, a description of the threat, a temporal profile specifying frequency of occurrence, a target (or targets) for the threat and a severity score for the (each target) are included in the	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise **SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR).

cyber threat data within the database, output the predicted future threat activity to one or more firewalls to improve their accuracy in correctly identifying cyber threats actually observed on the one or more computer networks to improve the accuracy of the apparatus and stochastic modeling of assessing financial loss from cyber threats on an ongoing basis;	Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
wherein execution of the computer program causes the computer system to perform, for each given threat, steps further comprising:	
modeling a set of past observed computer network cyber threat events to obtain an estimate of at least one model parameter;	
performing a Monte Carlo simulation of the given computer network cyber threat by:	
predicting future computer network cyber threat events using the at least one model parameter and a stochastic model using a projection of at least one model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable according to a predefined distribution and to use said at least one variable in the stochastic model and predicting a distribution of future computer network cyber threat events by repeating the simulation using a plurality of variables.	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

Note: Total claims: 15 and Independent claims: 3

EXHIBIT F	
Quantar's Preliminary Infringement Contentions	
US Patent No: 10122751 15/696,202	**Accused Instrumentalities**
Claim: 1	
1. A system comprising:	
one or more computers comprising one or more hardware processors;	
one or more computer-readable media storing instructions that, when executed by the one or more computers, cause the one or more computers to perform operations comprising:	
receiving, by the one or more computers, data indicating a list of observed computer-based threats including at least one selected from the group consisting of a virus, malware, a network intrusion, and a denial of service attack, with data for each threat identifying frequency of occurrence, which may include at least one period of time and corresponding frequency of occurrence for a given time window having a beginning and end;	
accessing, by the one or more computers, data specifying relationships between:	
(i) IT system infrastructures representing computing devices of an organization and a network connecting the computing devices and their physical and logical	

location, defined by information such as identity, name and category identity;	
(ii) system categories indicating characteristics of assets of the organization;	
(iii) operational processes of an organization, defined by identity, a name and a value in terms of a monetary value for a given time window having a beginning and end;	
(iv) mitigating actions representing the threat mitigation measures of the organization;	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
performing, by the one or more computers a plurality of simulations using a Monte Carlo method using the accessed data specifying relationships to predict a distribution of threat events, each simulation involving propagating data through stochastic modelling for a given time window having a beginning and end;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

modelling threat events using at least two different stochastic models and obtaining at least two different sets of model parameters, sampling, by the one or more computers, outcomes of the plurality of simulations generated using a Monte Carlo method according to the set of threat events within a series of temporal profiles, each having a beginning and end;	
sampling, by the one or more computers, a plurality of simulation outcomes of the plurality of simulations generated using a Monte Carlo method that include mitigating actions representing the threat mitigation measures of the organization for a series of given time windows, each having a beginning and end;	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
based on the sampled outcomes of the simulations, determining, by the one or more computers, measures of impact of the computer-related threats to the organization for a given time window having a beginning and end and providing, by the one or more computers and for output to a user, graphical representations of the determined measures of impact of the computer-based threats to the organization, for a given time window having a beginning and end, in a graphical user interface;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

the one or more computers further configured to;	
receive observed computer-based threat data;	
receive input data of the number of viruses contracted by period and the number of new viruses worldwide;	
extrapolating from the input data, using a Monte Carlo method, to predict future computer-based threat activity rates and types and;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
outputting said predicted future computer-based threat activity into the network and firewall logs, updating the firewall policy tree to define the action of accept or deny, according to the changes automatically made to the policy tree of rules in the sets of firewall rules, which in turn inserts updated rules into the firewall policy.	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
Claim: 9	
9. A method performed by one or more computers, the method comprising:	

receiving and accessing, by the one or more computers, data specifying relationships between:	
(i) IT system infrastructures representing computing devices of an organization and a network connecting the computing devices and their physical and logical location, defined by information such as identity, name and category identity;	
(ii) system categories indicating characteristics of assets of the organization;	
(iii) operational processes of an organization, defined by identity, a name and a value in terms of a monetary value for a given time window having a beginning and end;	
(iii) a list of observed computer-based threats including at least one selected from the group consisting of a virus, malware, a network intrusion, and a denial of service attack, with data for each threat identifying frequency of occurrence, which may include at least one period of time and corresponding frequency of occurrence for a given time window having a beginning and end;	
(iv) mitigating actions representing the threat mitigation measures of the organization;	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.

the one or more computers performing a plurality of simulations using a Monte Carlo method using the accessed data specifying relationships, each simulation involving propagating data through stochastic modeling for a given time window having a beginning and end;	
sampling by the one or more computers, outcomes of the plurality of simulations generated using a Monte Carlo method, for a given time window having a beginning and end;	
sampling by the one or more computers, outcomes of the plurality of simulations generated using a Monte Carlo method, that include mitigating actions representing the threat mitigation measures of the organization for a given time window having a beginning and end;	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
performing, based on the sampled outcomes of the simulations generated using a Monte Carlo method, determining, by the one or more computers, measures of impact of the computer-related threats to the organization for a given time window having a	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT

beginning and end and providing, by the one or more computers and for output to a user, graphical representations of the determined measures of impact of the computer-based threats to the organization, for a given time window having a beginning and end, in a graphical user interface;	Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
receive observed computer-based threat data;	
receive input data of the number of viruses contracted by period and the number of new viruses worldwide;	
extrapolating from the input data, using a Monte Carlo method, to predict future computer-based threat activity rates and types and;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
outputting said predicted future computer-based threat activity to one or more firewalls, to improve accuracy in identifying computer based threats on the one or more computer networks, strengthen their accuracy through the detection of anomalous firewall policy rules, into the network and firewall logs, updating the firewall policy tree to define the action of accept or deny, according to the changes automatically made to the policy tree of	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

rules in the sets of firewall rules, which in turn inserts updated rules into the firewall policy, wherein the method is performed by one or more computers comprising one or more hardware processors;	
one or more computer-readable media storing instructions that, when executed by the one or more computers, cause the one or more computers to perform operations comprising.	
Claim: 17	
17. A non-transitory computer-readable medium storing instructions that, when executed by the one or more computers, cause the one or more computers to perform operations comprising:	
receiving and accessing, by the one or more computers, data specifying relationships between:	
(i) IT system infrastructures representing computing devices of an organization and a network connecting the computing devices and their physical and logical location, defined by information such as identity, name and category identity;	
(ii) system categories indicating characteristics of assets of the organization;	
(iii) operational processes of an organization, defined by identity, a name and a value in terms of a monetary value for a given time window having a beginning and end;	
(iv) a list of observed computer-based threats including at least one selected from the group consisting of a virus,	

malware, a network intrusion, and a denial of service attack, with data for each threat identifying frequency of occurrence, which may include at least one period of time and corresponding frequency of occurrence for a given time window having a beginning and end;	
(iv) mitigating actions representing the threat mitigation measures of the organization;	**SERVICENOW 2** RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
the one or more computers performing a plurality of simulations using a Monte Carlo method, each simulation involving propagating data through stochastic modeling for a given time window having a beginning and end;	
sampling by the one or more computers using the accessed data specifying relationships, outcomes of the plurality of simulations for a given time window having a beginning and end;	
sampling by the one or more computers using the accessed data specifying relationships, outcomes of the	**SERVICENOW 2**

plurality of simulations that include mitigating actions representing the threat mitigation measures of the organization for a given time window having a beginning and end;	RiskLens Integration The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.
based on the sampled outcomes of the simulations, determining, by the one or more computers, measures of impact of the computer-related threats to the organization for a given time window having a beginning and end and providing, by the one or more computers and for output to a user, graphical representations of the determined measures of impact of the computer-based threats to the organization, for a given time window having a beginning and end, in a graphical user interface;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
the one or more computers further configured to;	
receive observed computer-based threat data;	
receive input data of the number of viruses contracted by period and the number of new viruses worldwide;	
extrapolating from the input data, using a Monte Carlo method, to predict future computer-based threat activity rates and types and;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT

	Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
outputting said predicted future computer-based threat activity to one or more firewalls, to improve accuracy in identifying computer based threats on the one or more computer networks, strengthen their accuracy through the detection of anomalous firewall policy rules, into the network and firewall logs, updating the firewall policy tree to define the action of accept or deny, according to the changes automatically made to the policy tree of rules in the sets of firewall rules, which in turn inserts updated rules into the firewall policy.	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

Note: Total claims: 20 and Independent claims: 3

EXHIBIT G	
Quantar's Preliminary Infringement Contentions	
US Patent Application No: 20180039922 15/231,131	**Accused Instrumentalities**
Claim: 1	
1. Apparatus for calculating economic loss from electronic threats capable of affecting computer networks, a network includes at least two interconnected	

networks and at least two IT systems, the threats including at least one electronic threat, and business processes operating on the IT systems, the apparatus including one or more computer processors and a computer readable memory coupled to the one or more computer processors in which programming code is stored, wherein the, one or more computer processors are configured pursuant to programming code in the computer readable memory to:	
predict for each electronic threat capable of affecting computer networks in which IT systems operate, future threat activity based on past electronic threat activity wherein the electronic threats include computer viruses, Trojan horses, computer worms, malware, malicious signed binaries, hacking, and denial of service attacks, to receive electronic threat data from a database, to extrapolate future electronic threat event frequency and to produce a profile of predicted electronic threat activity comprising a list of predicted electronic threats, and their expected frequency of occurrence, wherein the electronic threat data includes observed threats and, for each electronic threat, one or more targets for the electronic threat and a severity score for each target;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determine expected downtime of each system of the IT systems independence upon said predicted electronic threat activity including the severity scores and extrapolated future event frequency;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT

	Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determine economic loss for each of the business processes dependent on the downtimes of the IT systems, and;	
add economic losses for each business process to obtain a combined economic loss arising from the electronic threat activity.	
Claim: 13	
13. A method for calculating economic loss from electronic threats capable of affecting computer networks, a network includes at least two interconnected networks and at least two IT systems, the threats including at least one electronic threat, and business processes operating on the IT systems, the apparatus including one or more computer processors and a computer readable memory coupled to the one or more, computer processors in which programming code is stored, wherein the one or more computer processors are configured pursuant to programming code in the computer readable memory to:	
predict for each electronic threat capable of affecting computer networks in which IT systems operate, future threat activity based on past electronic, threat activity	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC)

wherein the electronic threats include computer viruses, Trojan horses, computer worms, malware, malicious signed binaries, hacking, and denial of service attacks, to receive electronic threat data from a database, to extrapolate future electronic threat event frequency and to produce a profile of predicted electronic threat activity comprising a list of predicted threats and their expected frequency of occurrence, wherein the electronic threat data includes observed threats and, for each electronic threat, one or more targets for the electronic threat and a severity score for each target;	can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determine expected downtime of each system of the IT systems independence upon said predicted electronic threat activity including the severity scores and extrapolated future event frequency;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determine economic loss for each of the business processes dependent on the downtimes of the IT systems, and;	
add economic losses for the business processes to obtain a combined economic loss arising from the threat activity.	
Claim: 16	

16. A computer readable memory storing a computer program which when executed by a computer system, causes the computer system to perform a method of calculating economic loss from electronic threats capable of affecting computer networks, the computer network comprising IT systems, wherein business processes operate on the IT systems, the method comprising:	
predicting future electronic threat activity based on historical electronic threat activity, for each electronic threat capable of affecting computer networks in which IT systems operate;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
to receive electronic threat data from a database, to extrapolate future electronic threat event frequency and to produce a profile of predicted electronic threat activity comprising a list of predicted electronic threats and their expected frequency of occurrence, wherein the electronic threat data includes observed threats and, for each electronic threat, one or more targets for the electronic threat and a severity score for each target;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

determining expected downtime of each system of the total IT systems in dependence upon said predicted electronic threat activity including the severity scores and extrapolated future event frequency;	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
determining economic loss for each of the business processes dependent on the downtimes of the IT systems, and;	
adding economic losses for each business process to obtain a combined economic loss arising from the electronic threat activity.	

Note: Total claims: 16 and Independent claims: 3

EXHIBIT H	
Quantar's Preliminary Infringement Contentions	
US Patent No: 16/129,820	**Accused Instrumentalities**
CLAIM 1.	
A system, comprising one or more networks comprising computing systems that are subject to a security policy, the security policy comprising breach parameters defining one or more events that are indicative of an electronic threat, the security policy breach parameters	

being associated with a remediation provision in a network security device policy for the computing systems and the network or networks;	
one or more data and traffic collecting devices, deployed within the network or networks, that collect entity information and monitor network data and traffic of the network or networks that is related to security information;	
samples network data and traffic and automatically detects occurrence of one or more of the events that are indicative of an electronic threat based on the network data and traffic;	
identifies electronic threats using a list of known threats stored in a database;	
produces observed electronic threat data, which includes a list of the observed electronic threats and their frequency of occurrence and stores the data in a database accessed by a threat assessment system that;	
automatically determines the breach parameters that apply for the one or more electronic threats that have been identified; and generates a remediation of network	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT

security device security parameters for the network or networks based upon predicted losses arising from the observed electronic threats.	Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
CLAIM 16.	
A method, comprising: establishing security parameters for an entity, the security parameters defining one or more events that are indicative of an electronic threat, the security policy breach parameters being associated with a remediation provision in a network security device policy of the entity	
automatically detecting occurrence of one or more of the events that are indicative of an electronic threat;	
automatically determining the breach parameters that apply for the one or more events that occurred; and	
causing a remediation of network security device security parameters determined based upon predicted losses arising from electronic threats.	**SERVICENOW 1;** ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT

	Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise
CLAIM 20.	
A system, comprising: one or more data and traffic collecting devices deployed within a network that collect entity information and monitor network data and traffic of the network that is related to security information, the network comprising computing systems that are subject to a security policy, the security policy comprising breach parameters defining one or more events that are indicative of an electronic threat, the breach parameters being associated with a remediation provision in a network security device policy for the computing systems and the network or networks;	
a threat analyzer and threat assessment system: automatically detects occurrence of one or more of the events that are indicative of an electronic threat based on the network data and traffic;	
	SERVICENOW 1;

automatically determines the breach parameters that apply for the one or more electronic threats; and generates a remediation of network security device security parameters for the network or networks based on predicted losses arising from the observed electronic threats.	ServiceNow Governance, Risk, and Compliance (GRC) can connect the business, security, and IT Risk management - Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise

EXHIBITS

SERVICENOW 1

ServiceNow Governance, Risk, and Compliance

The business and IT challenge

Managing risk and compliance with a manual, siloed and reactive work model is no longer effective as the global regulatory environment continuous to evolve, forcing changes across your organization. Changes driven by the need to: adopt new business models, establish new partner relationships, deploy new technologies, and address the increasing number of threats and cyber risks. Many enterprises have discovered that without an integrated view of risk it is virtually impossible to quickly assess the impact on their existing compliance obligations and risk posture of these changes.

Respond to business risks in real-time with ServiceNow

ServiceNow Governance, Risk, and Compliance (GRC) helps transform inefficient processes across your extended enterprise into an integrated risk program. Through continuous monitoring and automation ServiceNow delivers a real-time view of compliance and risk, improves decision making, and increases performance across your organization and with vendors. Only ServiceNow can connect the business, security, and IT with an integrated risk framework that transforms manual, siloed, and inefficient processes into a unified program built on a single platform.

- **Risk management** – Detect, and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise, and respond to critical changes in risk posture
- **Policy and compliance management** – Automate best practice lifecycles, unify compliance processes, and provide assurances around their effectiveness
- **Audit management** – Scope and prioritize audit engagements using risk data and profile information to eliminate recurring audit findings, enhance audit assurance, and optimize resources around internal audits
- **Vendor risk management** – Institute a standardized and transparent process to manage the lifecycle for risks assessments, due diligence, and risk response with business partners and vendors

Identify risks in real-time
Configure real-time business and IT service performance data, and identify vendor requirements to enable automated controls testing. Define thresholds as indicators for continuous monitoring of your extended enterprise

Increase performance
The Now platform CMDB, process designer, service mapping, and consistent and cross-functional workflow automation simplifies GRC processes and eliminates errors

Optimize internal audit productivity
Use of risk data and issues management enables effective audit project scoping, planning, and reporting while optimizing internal audit and compliance resources

Improve strategic planning and decision making
Fine-grained business impact analysis, task management, and contextual alignment with the CMDB on a single platform provides cross-functional visibility to identify, prioritize, and appropriately respond to risks

Automate third-party risk
Formalized vendor risk assessment and tiering process, improved visibility, and transparency save time and reduce vendor risk.

Extend your Servicenow investment
The single platform of engagement offers orchestration, easy integration, and data ingest and publication capabilities

Previous Topic Next Topic

RiskLens Integration

Store

Subscribe •••

The ServiceNow® GRC RiskLens API Integration application incorporates quantitative analysis results from RiskLens, based on the Factor Analysis of Information Risk (FAIR). Risk managers are provided more accurate and timely risk exposure awareness in monetary terms. Risk owners have an in-depth view of the risks affecting their enterprise with the tools to manage and mitigate them more effectively.

Install the RiskLens Integration

The RiskLens Integration application is used within the Risk Management application.

Before you begin