

CLAIMS

1. A method for protecting a computer asset, the method comprising:
 - receiving multiple signatures, wherein different signatures from the multiple signatures are specific for different types of computer assets;
 - identifying a particular signature from the multiple signatures, wherein the particular signature is specific for a particular type of computer asset, wherein the particular signature is code that causes a particular gateway to block an intrusion from reaching a particular computer asset that is of the particular type of computer asset, and wherein the particular computer asset has a particular asset context that is specific for the particular computer asset;
 - extracting the particular signature from the multiple signatures based on the particular asset context;
 - identifying a particular gateway that protects the particular computer asset; and
 - installing the extracted particular signature from the multiple signatures only on the particular gateway.
2. The method of claim 1, wherein the particular computer asset is a database system, and wherein the particular asset context describes a level of vulnerability of the database system, an identification of the database system, a hostname of a host computer on which the database system is running, and an operating system used by the database system.
3. The method of claim 1, wherein the particular asset is a database program, and wherein the particular asset context describes a level of vulnerability of the database program, an identification of the database program, a hostname of a host computer on which the database program is running, a database system used by the database program, and an operating system used by the database system.
4. The method of claim 1, further comprising:
 - performing a Natural Language Processing (NLP) analysis on a set of vulnerabilities to extract risk related information, wherein the set of vulnerabilities describes vulnerabilities that apply to the particular gateway, and wherein the risk related information includes a list of vulnerable network resources that are protected by the particular gateway and that are vulnerable to the intrusion.
5. The method of claim 1, wherein a vulnerability of the particular computer asset to the intrusion is from a set of identified vulnerabilities, and wherein the set of identified vulnerabilities are identified in a Common Vulnerability Exposure (CVE) listing that is generated by a third party that monitors vulnerabilities for multiple computer systems.
6. The method of claim 1, further comprising:
 - training a Deep Neural Network (DNN) to identify the particular gateway by inputting a known training signature and a known training asset context into the DNN; and
 - identifying the particular gateway by inputting the particular asset context and the extracted particular

signature into the trained DNN.

7. A computer program product comprising a computer readable storage medium having program code embodied therewith, wherein the computer readable storage medium is not a transitory signal per se, and wherein the program code is readable and executable by a processor to perform a method comprising:

receiving multiple Intrusion Prevention System (IPS) signatures, wherein different IPS signatures from the multiple IPS signatures are specific for different types of IPS gateways that protect different types of computer assets;

identifying a particular IPS signature from the multiple IPS signatures, wherein the particular IPS signature is specific for a particular type of computer asset, wherein the particular IPS signature is code that causes a particular IPS gateway to block an intrusion from reaching a particular computer asset that is of the particular type of computer asset, and wherein the particular computer asset has a particular asset context that is specific for the particular computer asset;

extracting the particular IPS signature from the multiple IPS signatures based on the particular asset context;

identifying a particular IPS gateway that protects the particular computer asset; and

installing the extracted particular IPS signature from the multiple IPS signatures only on the particular IPS gateway.

8. The computer program product of claim 7, wherein the particular computer asset is a database system, and wherein the particular asset context describes a level of vulnerability of the database system, an identification of the database system, a hostname of a host computer on which the database system is running, and an operating system used by the database system.

9. The computer program product of claim 7, wherein the particular asset is a database program, and wherein the particular asset context describes a level of vulnerability of the database program, an identification of the database program, a hostname of a host computer on which the database program is running, a database system used by the database program, and an operating system used by the database system.

10. The computer program product of claim 7, wherein the method further comprises:

performing a Natural Language Processing (NLP) analysis on a set of vulnerabilities to extract risk related information, wherein the set of vulnerabilities describes vulnerabilities that apply to the particular IPS gateway, and wherein the risk related information includes a list of vulnerable network resources that are protected by the particular IPS gateway and that are vulnerable to the intrusion.

11. The computer program product of claim 7, wherein a vulnerability of the particular computer asset to the intrusion is from a set of identified vulnerabilities, and wherein the set of identified vulnerabilities are identified in a Common Vulnerability Exposure (CVE) listing that is generated by a third party that monitors vulnerabilities for

multiple computer systems.

12. The computer program product of claim 7, wherein the method further comprises:

training a Deep Neural Network (DNN) to identify the particular IPS gateway by inputting a known training signature and a known training asset context into the DNN; and

identifying the particular IPS gateway by inputting the particular asset context and the extracted particular signature into the trained DNN.

13. The computer program product of claim 7, wherein the program instructions are provided as a service in a cloud environment.

14. A computer system comprising one or more processors, one or more computer readable memories, and one or more computer readable non-transitory storage mediums, and program instructions stored on at least one of the one or more computer readable non-transitory storage mediums for execution by at least one of the one or more processors via at least one of the one or more computer readable memories, the stored program instructions executed to perform a method comprising:

receiving multiple Intrusion Prevention System (IPS) signatures, wherein different IPS signatures from multiple IPS signatures are specific for different types of IPS gateways that protect different types of computer assets;

identifying a particular IPS signature from the multiple IPS signatures, wherein the particular IPS signature is specific for a particular type of computer asset, wherein the particular IPS signature is code that causes a particular IPS gateway to block an intrusion from reaching a particular computer asset that is of the particular type of computer asset, and wherein the particular computer asset has a particular asset context that is specific for the particular computer asset;

extracting the particular IPS signature from the multiple IPS signatures based on the particular asset context;

identifying a particular IPS gateway that protects the particular computer asset; and

installing the extracted particular IPS signature from the multiple IPS signatures only on the particular IPS gateway.

15. The computer system of claim 14, wherein the particular computer asset is a database system, and wherein the particular asset context describes a level of vulnerability of the database system, an identification of the database system, a hostname of a host computer on which the database system is running, and an operating system used by the database system.

16. The computer system of claim 14, wherein the particular asset is a database program, and wherein the particular asset context describes a level of vulnerability of the database program, an identification of the database program, a hostname of a host computer on which the database program is running, a database system used by

the database program, and an operating system used by the database system.

17. The computer system of claim 14, wherein the method further comprises:

performing a Natural Language Processing (NLP) analysis on a set of vulnerabilities to extract risk related information, wherein the set of vulnerabilities describes vulnerabilities that apply to the particular IPS gateway, and wherein the risk related information includes a list of vulnerable network resources that are protected by the particular IPS gateway and that are vulnerable to the intrusion.

18. The computer system of claim 14, wherein a vulnerability of the particular computer asset to the intrusion is from a set of identified vulnerabilities, and wherein the set of identified vulnerabilities are identified in a Common Vulnerability Exposure (CVE) listing that is generated by a third party that monitors vulnerabilities for multiple computer systems.

19. The computer system of claim 14, wherein the method further comprises:

training a Deep Neural Network (DNN) to identify the particular IPS gateway by inputting a known training signature and a known training asset context into the DNN; and

identifying the particular IPS gateway by inputting the particular asset context and the extracted particular signature into the trained DNN.

20. The computer system of claim 14, wherein the program instructions are provided as a service in a cloud environment.