

CLAIMS

What is claimed is:

1. A computer-implemented method for cybersecurity vulnerability management, the method comprising:

receiving, by a consortium blockchain network, a vulnerability report by a security specialist node indicating a cybersecurity vulnerability of a service provided by a service provider node;

determining, by the consortium blockchain network, whether the security specialist node is authorized to submit the vulnerability report to the consortium blockchain network, wherein the consortium blockchain network is private among participating entities, and wherein a consensus process is controlled by an authorized set of nodes;

providing, by the consortium blockchain network, access to the vulnerability report to an administrator node for verifying the cybersecurity vulnerability in the vulnerability report if it is determined, by the consortium blockchain network, that the administrator node is authorized to obtain the vulnerability report;

receiving, by the consortium blockchain network and from the administrator node, a vulnerability verification report indicating a verification of the cybersecurity vulnerability in the vulnerability report;

storing, by the consortium blockchain network, information of the cybersecurity vulnerability into a vulnerability record that is stored on the consortium blockchain network, wherein the information of the cybersecurity vulnerability is based on the vulnerability report and the vulnerability verification report;

providing, by the consortium blockchain network, access to the vulnerability record to the service provider node if it is determined, by the consortium blockchain network, that the service provider node is authorized to access the vulnerability record; and

receiving, by the consortium blockchain network and from the service provider node, a notification indicating a resolution to the cybersecurity vulnerability.

2. The method of claim 1, wherein the cybersecurity vulnerability comprises at least one of a software vulnerability or a hardware vulnerability.

3. The method of any preceding claim, wherein determining, by the consortium blockchain network, that the administrator node is authorized to obtain the vulnerability report is done in response to receiving, by the consortium blockchain network and from the administrator node, a request to obtain the vulnerability report.

4. The method of any preceding claim, wherein determining, by the consortium blockchain network, that the service provider node is authorized to access the vulnerability record is done in response to receiving, by the consortium blockchain network and from the service provider node, a request to access the vulnerability record.

5. The method of any preceding claim, wherein the vulnerability report is received by the consortium blockchain network from a client device, and wherein the method further comprises:

receiving, by the consortium blockchain network and from the service provider node, a request to reward a consortium blockchain account of the client device; and

in response to receiving the request from the service provider node, providing, by the consortium blockchain network, a digital token as a reward to the consortium blockchain account of the client device.

6. The method of any preceding claim, further comprising:

in response to receiving the notification from the service provider node, storing, by the consortium blockchain network, the resolution to the cybersecurity vulnerability into the vulnerability record; and

providing, by the consortium blockchain network, access to the vulnerability record to a service user of the service.

7. The method of any preceding claim, wherein the resolution to the cybersecurity vulnerability comprises at least one of the following: a software patch, or a hardware replacement.

8. An apparatus for cybersecurity vulnerability management, the apparatus comprising a plurality of modules for performing the method of any one of claims 1 to 7.

9. A system for cybersecurity vulnerability management, comprising:
one or more processors; and
one or more computer-readable memories coupled to the one or more processors and
having instructions stored thereon that are executable by the one or more processors to
perform the method of any one of claims 1 to 7.