

CLAIMS

1. A system for detecting threats comprising:
 - a first server computing device included in a communications network to:
 - provision components for deployment as a honeynet network in the communications network, based on provisioning data stored at the first server computing device that is not accessible by the provisioned components once deployed as the honeynet network, the honeynet network to monitor unauthorized network traffic attempting to access a service executing within the honeynet network, the provisioned components of the honeynet network comprising:
 - a processing device to log the unauthorized network traffic;
 - a gateway device to receive a first portion of the unauthorized traffic and generate a first set of logs corresponding to the unauthorized traffic;
 - a honeypot to receive a second portion of the unauthorized traffic, wherein the honeypot executes an instance of the service, and wherein the honeypot monitors the unauthorized network traffic of the service and generates a second set of logs corresponding to the monitored unauthorized traffic; and
 - a second server computing device to automatically configure the gateway device, the processing device, and the honeypot based on configuration data stored at the second server, wherein the configuration data is not accessible by the first server.
2. The system of claim 1, wherein the provisioning data includes at least one of application programming interface keys, secure shell keys, and authentication parameters used during the provisioning of the one processing device, the gateway device, the honeypot, and the second server.
3. The system of claim 1 or 2, wherein the configuration data includes an application and one or more files defining instructions for installing the application and wherein to automatically configure the processing device, the gateway device, and the honeypot comprises:
 - installing the application on at least one of the processing device, the gateway device, and the honeypot based on the instructions.

4. The system of any one of claims 1 to 3, wherein the service emulates a behavior of an identical service executing on a network device of the communications network to attract the unauthorized network traffic to the honeynet network.
5. The system of any one of claims 1 to 4, wherein the processing device is further configured to identify a threat from the unauthorized network traffic and prioritize the threat based on a number of times the threat is identified from the network traffic.
6. The system of any one of claims 1 to 5, wherein the processing device is further configured to provide access to the first set of logs and the second set of logs to at least one network device of the communications network.
7. The system of any one of claims 1 to 6, wherein the honeynet network is separate and external to the communications network.
8. A method for detecting threats comprising:
 - provisioning components for deployment as a honeynet network in a communications network based on provisioning data that is not accessible by the provisioned components once deployed as the honeynet network, the honeynet network to monitor unauthorized network traffic attempting to access a service on a network device of a cluster of network devices deployed within the communications network, the provisioning including:
 - provisioning a processing device to log the unauthorized network traffic;
 - provisioning a gateway device to receive a first portion of the unauthorized traffic and generate a first set of logs corresponding to the unauthorized traffic;
 - provisioning a honeypot to receive a second portion of the unauthorized traffic, wherein the honeypot executes an instance of the service, and wherein the honeypot monitors the unauthorized network traffic of the service and generates a second set of logs corresponding to the monitored unauthorized traffic; and
 - provisioning a second server to automatically configure the processing device, the gateway device, and the honeypot based on configuration data stored at the second server, wherein the configuration data is not accessible by the first server.

9. The method of claim 8, wherein the provisioning data includes at least one of application programming interface keys, secure shell keys, and authentication parameters used during the provisioning of the one processing device, the gateway device, the honeypot, and the second server.
10. The method of claim 8 or 9, wherein the configuration data includes an application and one or more files defining instructions for installing the application and wherein to automatically configure the processing device, the gateway device, and the honeypot comprises:
installing the application on at least one of the processing device, the gateway device, and the honeypot based on the instructions.
11. The method of claim any one of 8 to 10, wherein the service emulates a behavior of an identical service executing on a network device of the communications network to attract the unauthorized network traffic to the honeynet network.
12. The method of any one of claims 8 to 11, wherein the processing device is further configured to identify a threat from the unauthorized network traffic and prioritize the threat based on a number of times the threat is identified from the network traffic.
13. The method of any one of claims 8 to 12, wherein the processing device is further configured to provide access to the first set of logs and the second set of logs to at least one network device of the communications network.
14. The method of any one of claim 8 to 13, wherein the honeynet network is separate and external to the communications network.
15. A non-transitory computer readable medium encoded with instructions for performing the method of any one of claims 8 to 14, the instructions executable by a processor.