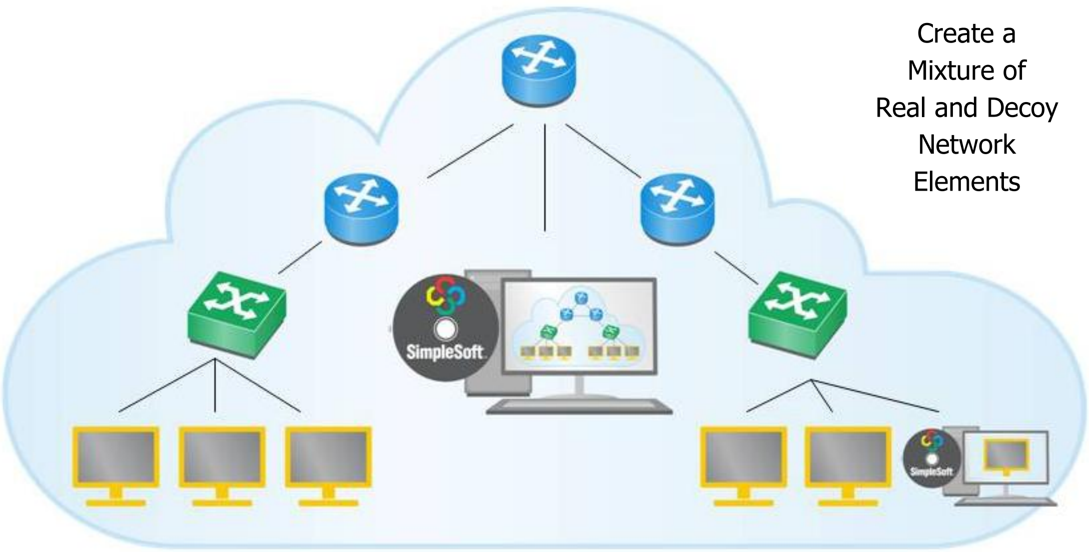
SimpleIoTDecoy ™

A Deceptive Honeypot for Intrusion Detection

SimpleSoft

Simplifying
Network & IoT
Management



Create a
Mixture of
Real and Decoy
Network
Elements

Overview

SimpleIoTDecoy is an easy to use, software based device simulator that acts as an **intelligent honeypot** to detect intrusions, while **deceptively** appearing like just another device on your network.

SimpleIoTDecoy supports many of the common IoT and network management protocols like **MQTT**, **CoAP**, **Modbus, BACnet, HTTP/s, SNMP, Telnet, SSH, IPMI, TL1, and Netconf**. The Decoy can **"learn"** from existing devices to duplicate them and then run inside your intranet on computers/VMs using unused IPs to create a mixture of real and simulated devices. SimpleIoTDecoy, using patented technology, will then simply listen for incoming requests and respond to them appropriately based on the learnt data and log the interaction. It will silently **flag intrusions** when it receives requests from unknown entities or receives requests that are different from the ones it is expecting. White lists of known entities and requests can get automatically populated by accepting requests during a specified interval or created manually. Request fingerprinting is used to distinguish between similar requests sent from known entities that have been compromised. Both IPv4 and IPv6 protocols are supported and SimpleIoTDecoy can run on physical as well as virtual machines.

Benefits

The **SimpleIoTDecoy** adds one more **security tool** to an **IT department's** arsenal for **intrusion detection** within the intranet. When hackers infiltrate the intranet, they typically scan the network to discover the devices connected to it. SimpleIoTDecoy devices will show up alongside real devices in the scan and appear just as real. The Decoys will respond back to queries like real devices, while silently keeping a log of the requests made and raise an alarm to identify the compromised servers used to send the requests. The logs can be used to run forensics and analyze the mode of operation of the intruders **without putting any real resources at risk**. Intrusion alerts can be forwarded to the main NMS in the form of SNMP Traps and syslog messages. The logs can also be used to train machine learning algorithms for intrusion detection and for creating signatures.

Operation

Only a few simple steps are required to start using the **SimpleIoTDecoy**. They are:

- Use the built-in **learner** utilities to record packet exchanges from real devices.
- Use this learnt data as a template to create decoys and assign them unused IPs on your intranet.
- Wait for SimpleIoTDecoy to detect intrusions and send alerts. Examine logs to run forensics.

System Requirements

- 64bit Linux OS.

SimpleSoft Inc.
257 Castro Street
Suite 220
Mountain View
CA 94041
650.965.4515
650.965.4505 fax
sales@simplesoft.com
www.simplesoft.com