GAMBIT COMMUNICATIONS CASE STUDY

MIMIC NetFlow Simulator helps Seceon Develop Innovative Data Center/Cloud Security Solution

"MIMIC has been a tremendous help in aiding us to simulate different kinds of data center traffic with thousands of Hosts, tens of Switches and Routers. It provided a large lab environment which was otherwise impossible for us to build."

Chandra S. Pandey
Founder and CEO

Seceon dashboard showing Adaptive Visualization of Assets along with Holistic Threat Detection and Dynamic Security Posture using MIMIC Simulator.

If you are a startup and have limited capital, how do you create a large network environment for testing your application? For Seceon testing their Data Center and Cloud Security solutions by leveraging against a large data center is very important. Seceon solution comprises of Centralized Fast and Big Data Analytics and Policy Engine (APE) based on real-time Threat Detection and Dynamic Security Posturing with Innovative Command and Control Engine (CCE) for on-demand Feature Extraction aided by an advanced cyber security Machine Learning Engine. Seceon targets enterprises with public, private and hybrid cloud data centers and the solution can be deployed in-house or utilize Seceon SaaS solution.

Challenges:
The Seceon solution relies on a number of sources to detect security breaches, anomalies and Advanced Persistent Threats (APT). One such source is NetFlow generated by routers and switches installed on every rack in the datacenter.

Seceon needed to setup a large environment with thousands of routers and switches, along with many servers. Being a start-up, it was cost prohibitive for them to build a lab or get access to a large lab on their own. Instead of building a large lab, they considered the option to use an enterprise grade network simulator. They researched and evaluated a variety of hardware and software based simulators and decided on MIMIC SNMP/NetFlow Simulator that supported all the technical features they needed, fit in their budget and was extremely flexible to simulate various customers' environments.

Solution:
Seceon was immediately able to deploy **MIMIC SNMP and NetFlow Simulator** and create a virtual lab full of SNMP; Cisco® NetFlow, IPFIX, NBAR, NBAR2 and Cisco Flexible NetFlow data based devices. They can simulate different kinds of data center traffic, including port scanning, IP scanning, database access, accessing malicious blacklisted sites, communication between applications clusters and network segments. MIMIC Simulator helped them to completely test their data center/cloud security solution.

MIMIC NetFlow Simulator generates a variety of flows (at a rate of 2 million flows/sec). Seceon engineers have complete control over precisely generated Flowsets. They can easily verify that their solution correctly handles different network conditions.

MIMIC Simulator allows Seceon to test and refine their security solution without having to invest in routers, switches and thousands of hosts or any traffic generation tools.

MIMIC Simulator creates a virtual data center to test the detection of various security breaches for Seceon's Dynamic Security Posture (DSP) Platform.

For more information:
Please contact **Gambit Communications**: info@gambitcomm.com **www.gambitcomm.com**