Rogue Device Detection

offerings.infotex.com

The **infotex** Rogue Device Detection (RDD) service can be thought of as a steppingstone to a Network Access Control (NAC) system. The primary distinction is that our service is modeled to be unintrusive by notifying your institution, but not blocking or preventing anything. This provides crucial visibility without the headache of the restrictive controls and cost concerns of a NAC.

How does RDD work?

- During initial setup, **infotex** will ask for an approved list of devices for a Client's network. This can be provided to us, or we can harvest the list during a tuning period.
- Once the approved list of devices is created, the system will be turned on.
- When any new device that connects to your network it is tracked by its MAC address as its primary identifier. This cuts down on the system becoming noisy if a device changes IP, hostname, etc.
- An email is sent to you via our ticketing system.
- If the new device is known or is expected, you can respond to the email to have it added to your approved device list.
- If the device is determined to be Rogue, then no action is necessary via our system. The device will remain Rogue and the RDD service will report it anytime the device is on your network going forward.
- If you wish, we can even Put-A-Watch on the device to gather more information.

How RDD helps your SIEM function better:

infotex prides itself on being an extension of your incident response / IT team, so if you utilize the RDD system properly you will give our team additional context, and generally increase awareness of our 24/7 Data Security Analysts. This also has the added benefit of training our system and DSAs to identify devices and provides additional real-world context. Thus, making your SIEM work as effectively as possible!

If you are interested in our Rogue Device Detection, SIEM, or any of our other services, please visit:

offerings.infotex.com