IoT Devices Exfiltrating Data

Industry: Oil and Gas

Attacker Objective

Use unsecured IoT devices to gain access to network

Background

An oil and gas facility had two high-tech exercise bicycles connected to the internet and communicating through insecure methods. These were not segmented from corporate IT resources and thus presented the attacker with a network path to the organization's critical assets.

Arista NDR identified that the two exercise bikes were sending unencrypted HTTP traffic to the internet and used basic authentication (a weak authentication method that exposes the username and password). Both machines were sitting on the corporate network and exfiltrating data out to the internet. Additionally, they appeared unpatched, leaving the facility wide open to attack.

The firm's IT and security teams were completely unaware of these devices being on the network since existing security and configuration management tools were blind to these unmanaged IoT devices.

Arista NDR detected this threat even though:

- It existed in a blind spot, and no one knew these devices were network-enabled.
- The organization had IoT devices with no inherent security and manageability using an insecure protocol for outbound communications.
- It had only basic user authentication that was easily exploited for malicious attacks.

Why Arista NDR?

Many IoT devices are inherently insecure, thus providing an opportunity for an attacker to gain a foothold into the enterprise network. Given the IT and security teams didn't know these devices were on the network, they were blind to the risk until receiving a notification from Arista NDR.

Arista NDR continuously monitors enterprise devices, users, and applications wherever they are, even as IP addresses change, while maintaining a forensic record of past activities.

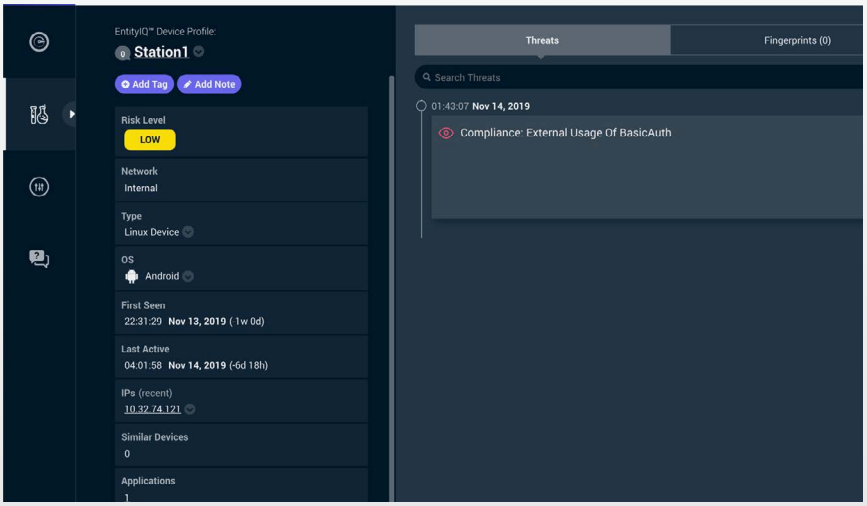

Fig 1: The device detail page in the Arista NDR platform shows an EntityIQTM profile of an IoT device triggering an HTTP Basic Authentication adversarial model.

Arista NDR automatically looks for weak and insecure authentication mechanisms, use of clear-text credentials, and sensitive data leaving the network. These activities triggered an adversarial model in the Arista NDR platform, which alerted the security team about the insecure IoT devices.