IoT Devices Exfiltrating Data

An oil and gas facility had two high-tech exercise bicycles that were 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.

Awake 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 to be un-patched, 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.

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

Many devices on the Internet of Things are inherently insecure, thus providing an opportunity for an attacker to gain a foothold on a company 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 Awake.

Industry

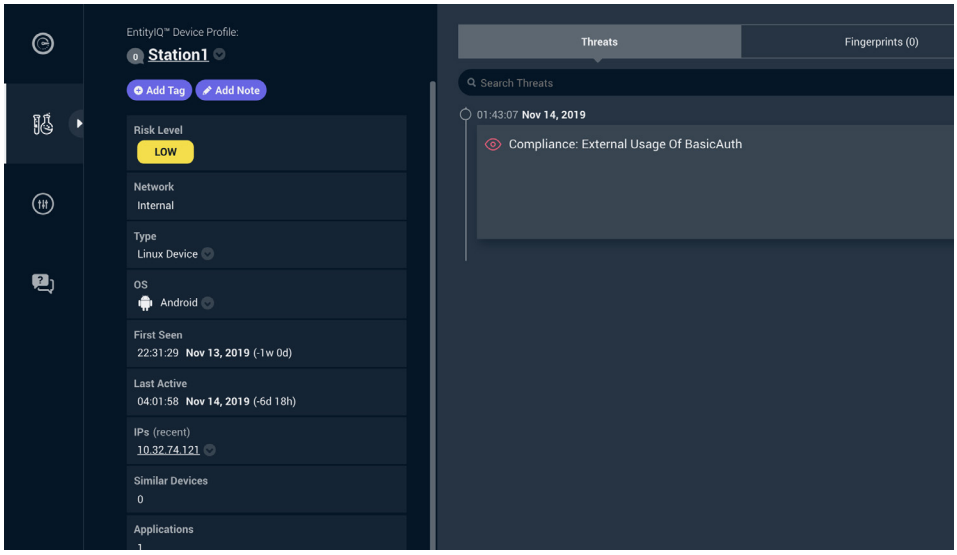
Oil and Gas

Attacker Objective

Use unsecured IoT devices to gain access to network

Awake detected this threat as:

- Existing in a blind spot, as no one knew these devices were network-enabled.
- A manifestation of Internet of Things devices with no inherent security and manageability.
- Outbound communications using an insecure protocol.
- Basic user authentication that can easily be exploited for malicious attack.



The device detail page on Awake's platform shows an EntityIQ™ profile of an IoT device triggering a HTTP Basic Authentication adversarial model..

For additional information about Awake please visit awakesecurity.com

AWAKE