DEPLOYMENT GUIDE

Collecting IPAM Metadata from a NIOS Source

BloxOne Threat Defense

Table of Contents

Overview

BloxOne Threat Defense can enrich threat alerts with IPAM data from an Infoblox Grid. When IPAM data is shared with BloxOne Threat Defense, the incident responder will see the device name and device type (DHCP Fingerprint) embedded in the security alert.

	THREAT	CONFIDENCE	QUERY	DEVICE NAME	DEVICE IP	MAC ADDRESS	DHCP FINGERPRINT
☐	LOW	LOW	api2.branch.io.	DANIELs-iPad	192.168.1.253	a4:f1:e8:98:78:5f	Apple iPod, iPhone or iPad

A BloxOne Threat Defense Security Alert.

Requirements

The following are required for this solution:

1. BloxOne on-prem host (OPH)
    - Cloud Data Connector (CDC) Service running on the OPH
2. NIOS Grid with IPAM, DHCP and Object Tracking enabled

The CDC will periodically poll the NIOS grid for IPAM information via a REST command. The CDC will then transfer IPAM metadata to the CSP via SCP. In the CDC configuration, NIOS will be the source, BloxOne will be the destination, and the traffic flow configuration will specify the collection of IPAM metadata.

Configuration Guide

This guide will not cover installation of the on-prem host. Please see Deploying Hosts for BloxOne DDIfor details on OPH installation.

You must enable the NIOS Object Change Tracking feature. When you enable this feature, the appliance tracks the changes that are made to NIOS objects and periodically synchronizes changed objects. For instructions on how to enable this feature, see Enabling Object Change Tracking in the Infoblox NIOS documentation portal.

Object Change Tracking will increase the CPU load of the grid master. Please consult Infoblox Support or your account SE if your grid master is resource constrained.

The following information is transferred from the Default DNS View to BloxOne:

- Hostname
- DHCP Fingerprint

- MAC Address or IPv6 DUID
- Usernames for:
    - Microsoft Active Directory
    - Cisco ISE
- DNS Appliance Name - hostname/IP (NIOS, DFP)
- DNS View

To configure the Data Connector to send NIOS IPAM metadata to the CSP, complete the following:

1. Log in to the Cloud Services Portal.
2. Click **Manage** -> **Data Connector**.
3. Select the **Source Configuration** tab.
4. Create a new **NIOS source** if you do not already have one. For more information on creating NIOS sources, see Adding a NIOS Source Configuration.
5. Select the **Traffic Flow Configuration** tab.
6. **Create** a new **Traffic Flow Configuration**. For more information on creating Traffic Flows, see Creating Traffic Flows.
7. In the **SELECT CONFIGURATION** section, complete the following:
    - Expand the **Source Configuration** section and select your NIOS source.
        - Click the checkbox for **IPAM Metadata/DHCP Lease Information**.
    - Expand the **Destination Configuration** section and select **BloxOne Cloud Destination.**
8. Click **Save & Close** to save the newly updated configuration.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com