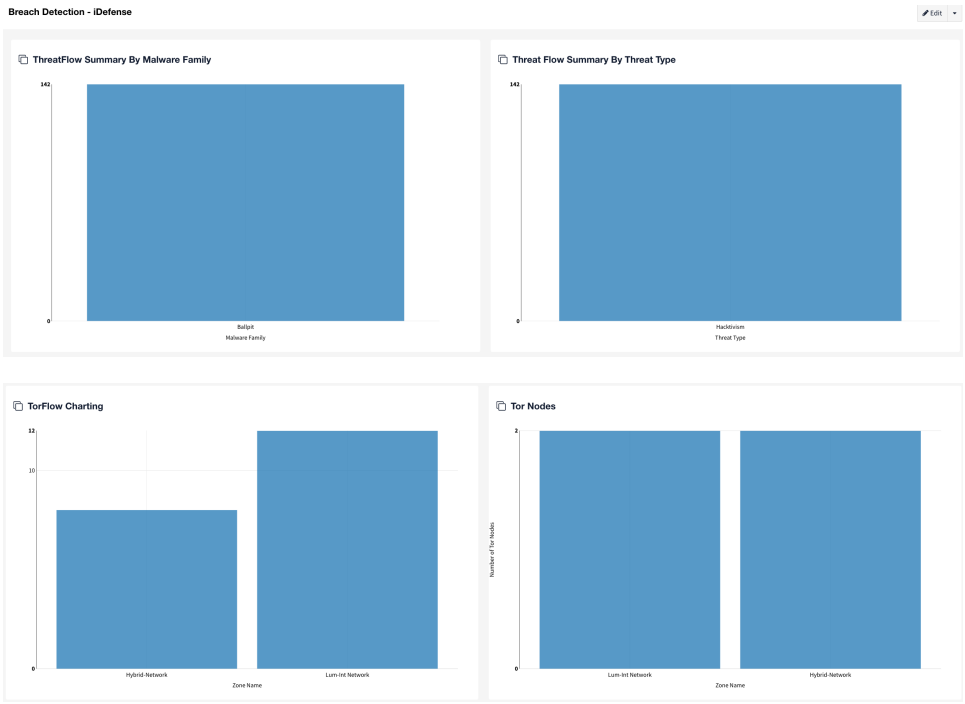
Breach Detection

The Breach Detection dashboards, Breach Detection and Breach Detection - iDefense, are powered primarily by the iDefense, and Emerging Threats integrations (which is open source), but are also affected by the Tor, ISC Port and NetFlow feeds, enable you to monitor all Lumeta zones relative to security threats.

1. **Both Dashboards** - In Lumeta, both dashboards present data in these categories:
    a. Zombie Devices
    b. Tor Nodes
    c. TorFlow Charting
    d. Nefarious Ports

2. **Breach Detection Dashboard:** The Breach Detection dashboard also uniquely presents data fed by the Emerging Threats integration in the ThreatFlow Charting widget.

3. **Breach Detection Dashboard - iDefense:** Presents unique data from iDefense such as Threatflow by Malware Family and Threatflow by Threat Type.



Auto-Refresh

Refresh your browser to update *all widgets* on the Breach Detection dashboard. Or, set an interval at which to automatically refresh *a selected widget* on the dashboard (Edit > Gear icon > Edit Widget Settings).

Zombie Devices

Are your network's active security controls preventing communications to known zombie and command-and-control (C2) networks and servers? This widget helps you watch in real time for exfiltration to known bad servers and networks that were identified via open-source and closed-source intelligence feeds and repositories.

If CTP finds access to C2/Zombie machines, the following may be occurring:

- Firewall rules are not effective at limiting outbound sessions over protocols known to be at-risk.
- Firewalls/NGFW/IPS/DLP solutions are not effective at limiting or blocking access to known bad networks or servers.
- Given that one or more egress points let traffic out, security architecture is not uniform across the enterpri

ThreatFlow Charting

About ThreatFlow

ThreatFlow has the following dependencies and requirements:

1. The threat categories associated with this ThreatFlow Charting widget will display only if your organization has a subscription to Emerging Threats Pro. Without this subscription, the widget will show all of the threat conversations between a company's internal IPs and zombie/threat IPs i*n a single category*.
2. Your organization must hav a *single source* of NetFlow data such as Gigamon NetFlow because Lumeta can only receive NetFlow from a single source. If you have multiples, consider using a NetFlow aggregator.
3. NetFlow data must be directed to your Lumeta Command Center.

Contact your Solutions Architect and Support if you need assistance with any of these items.

The ThreatFlow view shows the intersection of threat intelligence feeds and NetFlow data.

Nefarious Ports Summary

This dashboard view is designed to highlight any devices found with open known-vulnerable ports. After nefarious ports candidate devices have been identified, your organization is advised to manually validate any exploit activity and take action to remediate compromised assets.