



ThreatIQ and Anomaly Detection

THREATIQ, GEOBLOCKING AND ANOMALY DETECTION



Aviatrix ThreatIQ



Block Threats Based on Geographic Location

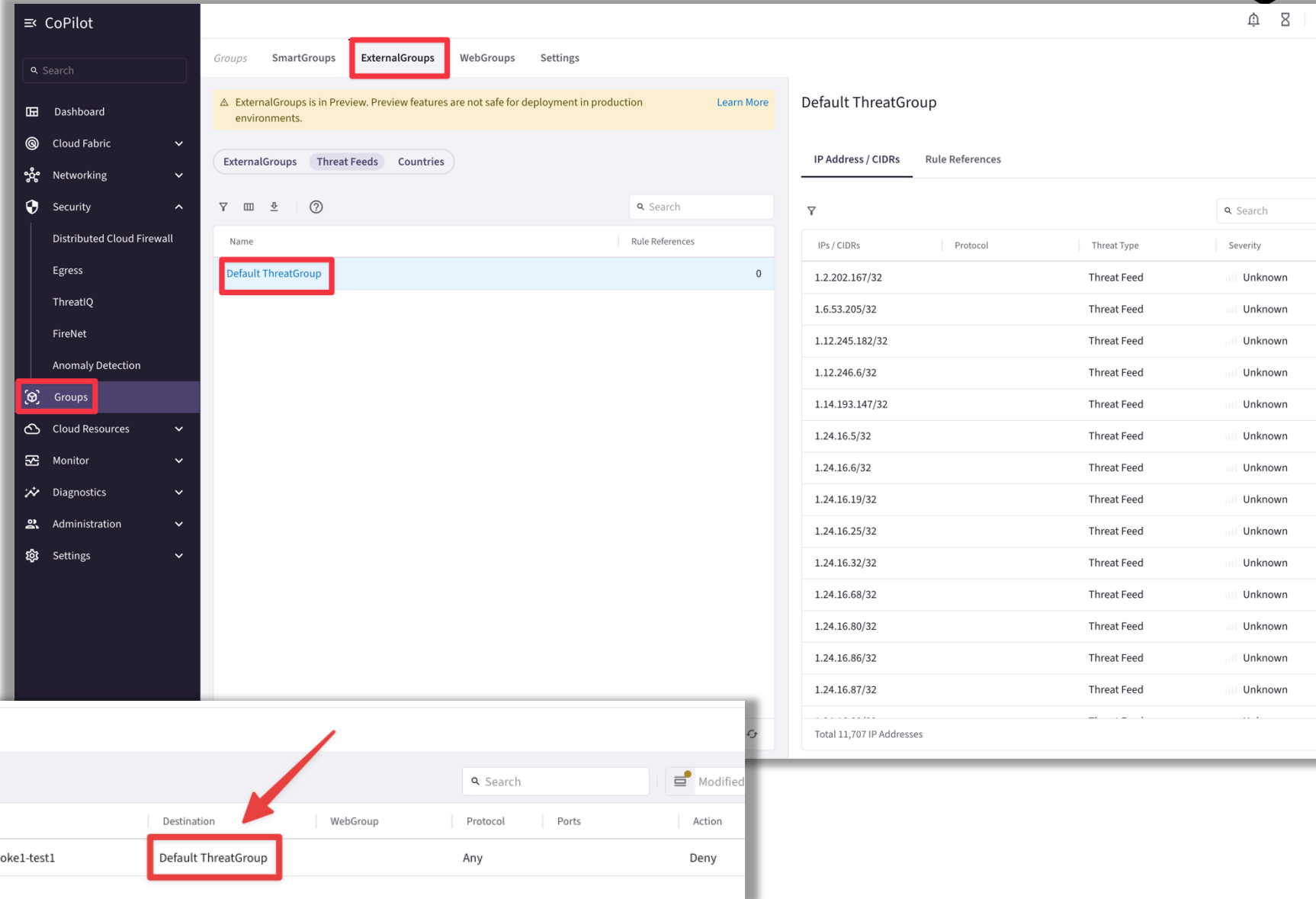
Default ThreatGroup

ProofPoint Database

- The **Default ThreatGroup** can be used to ensure that traffic meeting the ThreatGroup criteria is blocked
- The **Default ThreatGroup** is regularly updated with data from *ProofPoint Global Threat Defense Database* (every 30 min)
- The Default ThreatGroup references the complete list of all the Malicious IP addresses.

Note:

- You cannot have a ThreatGroup as both source and a destination in a DCF rule



The screenshot displays the Aviaatrix CoPilot interface. On the left, the 'Groups' menu item is highlighted. The main panel shows the 'ExternalGroups' tab, where the 'Default ThreatGroup' is listed. A red box highlights the 'Default ThreatGroup' entry. To the right, a table titled 'Default ThreatGroup' lists various IP addresses and their associated threat types and severities.

IPs / CIDRs	Protocol	Threat Type	Severity
1.2.202.167/32		Threat Feed	Unknown
1.6.53.205/32		Threat Feed	Unknown
1.12.245.182/32		Threat Feed	Unknown
1.12.246.6/32		Threat Feed	Unknown
1.14.193.147/32		Threat Feed	Unknown
1.24.16.5/32		Threat Feed	Unknown
1.24.16.6/32		Threat Feed	Unknown
1.24.16.19/32		Threat Feed	Unknown
1.24.16.25/32		Threat Feed	Unknown
1.24.16.32/32		Threat Feed	Unknown
1.24.16.68/32		Threat Feed	Unknown
1.24.16.80/32		Threat Feed	Unknown
1.24.16.86/32		Threat Feed	Unknown
1.24.16.87/32		Threat Feed	Unknown

Below the table, it states 'Total 11,707 IP Addresses'.

At the bottom, a screenshot of the 'Rules' tab in the Distributed Cloud Firewall shows a rule named 'PSF-Deny-Rule-from-aws-us-east-1-spoke1-test1'. The 'Destination' field is set to 'Default ThreatGroup', which is highlighted with a red box and a red arrow.

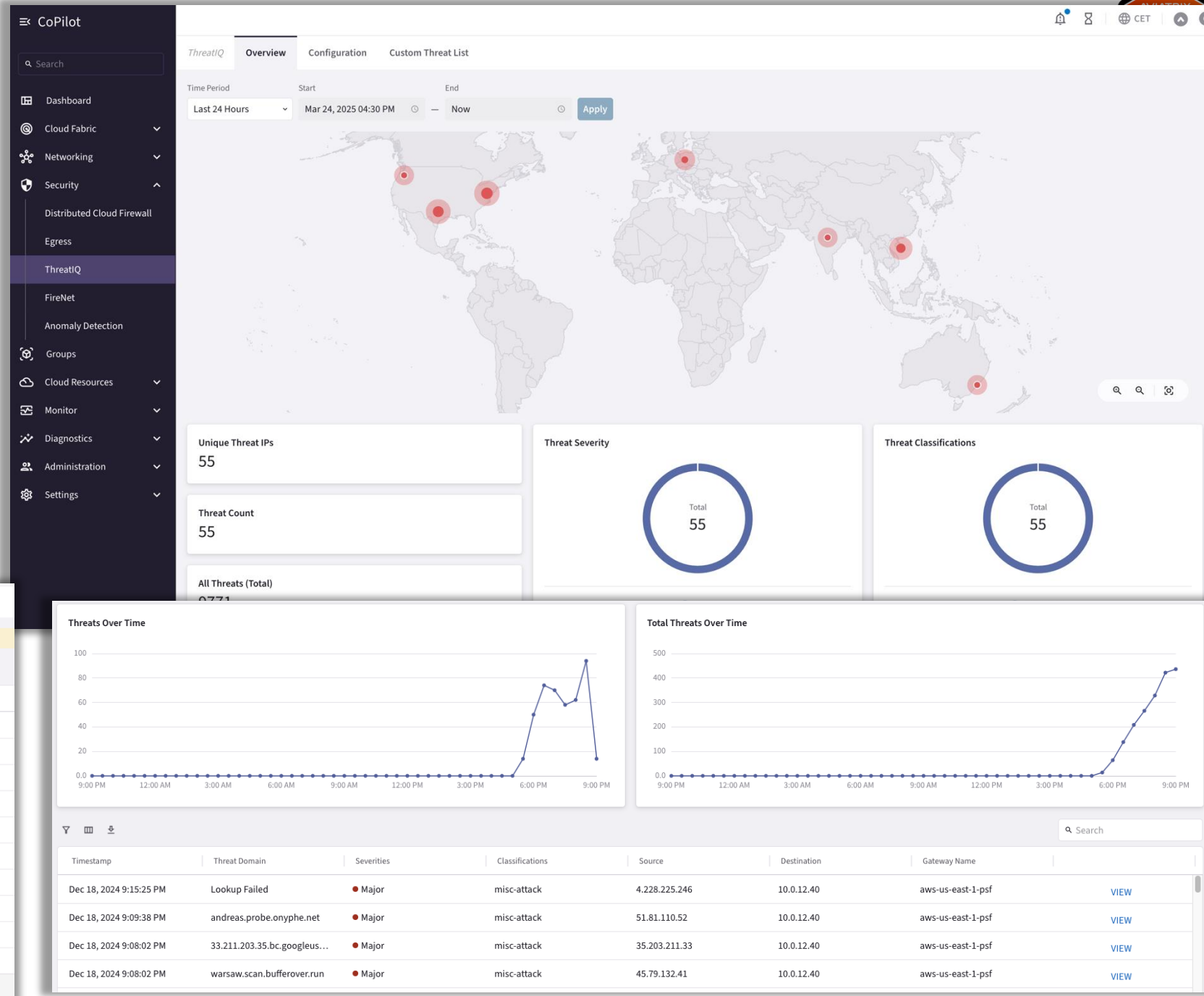
ThreatIQ

Overview Tab

- Shows a geographical map with the approximate locations of known malicious IPs that have communicated with your network within the specified time period selected.
- You can view the severity level of detected threat IPs and their associated attack classifications (as categorized by the well-known threat IPs DB).

Geoblocking Tab

- Block traffic coming from other countries





Network Behavior Analytics

Aviatrix Anomaly Detection





**Next: Security and Operational
Visibility**