

# Leveraging Commercially Available Data to View, Analyze, and Investigate Beyond the Traditional Security Perimeter

## THE PROBLEM

- > Typical network defense has limited visibility beyond the boundary
- > Cannot follow to the second hop and beyond, requiring correlated CTI to identify malicious infrastructure
- > More data, more answers. Also, more complicated aggregation, correlation, and analysis
- > Data sources can be challenging to acquire
- > Proficient analysts can be challenging to acquire

## THE APPROACH

- > Extend visibility beyond the boundary and enrich with passively acquired data
- > Focus on the greater public Internet for ingress and egress connections to a network of interest
- > Provide ShadowView analyst a platform that allows for quick and precise movements to respond to RFIs
- > Aggregate data sources that are hard to acquire
- > Remove analyst hiring, training, and retention burdens

