Analyzing “Badness”

Chapter Use Case: Crunching AlienVault IP Reputation Data

Dissecting The “IP Address”

32-bit integer (“how does your computer see an IP address?”) + machine info

Part of a subnet / logical layout / MAC addresses, perhaps has a hostname (DNS)

Larger context: part of a global network organized by ASNs (BGP)

Lager context: Has a physical location

Mapping Outside the Continents

USE CASE: Visualizing AlienVault ASN data (force-directed network graphs of malhost ASN groupings)