



FINANCIAL SERVICES

The following example describes the situation we encountered at a financial services company.

The network environment at the financial services company consists of 40 servers, 2 firewalls, 4 Snort IDS systems, and dozens of Cisco routers and switches. Their network architecture is designed to have all of the network communication run through their main Cisco router.

We installed the TAC software on an existing Linux server on their network and collected the previous day's NetFlow logs from their main Cisco router. When we ran the TAC against the logs we found three threats to their network.

1. Users were in places on the network that they were not authorize to access
2. Internal servers that were not authorized to be on the network that were being accessed from the Internet
3. Areas where the network was not properly divided for security

These findings represent internal and external threats to their network that went undetected by their existing firewall and IDS systems. The reason the threat were undetected is because their firewalls and IDS systems were not programmed with specific rules to look for these types of threats.

RazorThreat's TAC found these threats as a result of looking at all of the communication internal to and external to the network. The TAC provides a second order analysis on all of the data crossing their network finding threats and errors and omissions that their existing perimeter and point solutions are not capable of identifying.