Background

Big Marketing is an international marketing company employing a large staff of marketing executives who create and manage advertising and public relations campaigns for clients. Big Marketing has an internet research staff that stays current on the latest business, consumer and entertainment trends, searches for new markets, and comes up with ways to make Big Marketing's clients stand out from the crowd. In addition, Big Marketing operates web sites for selected clients.

You work as the Big Marketing computer network manager, ensuring that Big Marketing networks are up and running for both the Internet-facing web services and the internal workforce. This responsibility encompasses the full range of maintaining current operations, planning for future needs, and securing and defending network assets against threats.

Mini-Challenge Questions

In this VAST Challenge 2013 Mini-Challenge, your job is to understand events taking place on your networks over a two week period. To support your mission, your choice of visual analytics should support near real-time situation awareness. In other words, as network manager, your goal for your department is to notice network events as quickly as possible.

MC3.1 – Provide a timeline (i.e., events organized in chronological order) of the notable events that occur in Big Marketing's computer networks for the supplied data. Use all data at your disposal to identify up to twelve events and describe them to the extent possible. Your answer should be no more than 1000 words long and may contain up to twelve images.

MC3.2 – Speculate on one or more narratives that describe the events on the network. Provide a list of analytic hypotheses and/or unanswered questions about the notable events. In other words, if you were to hand off your timeline to an analyst who will conduct further investigation, what confirmations and/or answers would you like to see in their report back to you? Your answer should be no more than 300 words long and may contain up to three additional images.

MC3.3 – Describe the role that your visual analytics played in enabling discovery of the notable events in MC3.1. Describe whether your visual analytics play a role in formulating the questions in MC3.2. Your answer should be no more than 300 words long and may contain up to three additional images.

Data Sources

The data under investigation spans a two week period. Data for both weeks is now available.

You have four sources of data and information at your disposal in order to characterize what is happening on the network:

1. Network description
2. Network flow data (netflow data)
3. Network health and status data (Big Brother data)

4. Intrusion Protection System data.
5. Questions to the Big Marketing corporate office

1. Network Description.
The Big Marketing network description for Week 1 is included with the Answer Sheet and Data Descriptions download. The updated network description reflecting the network configuration in Week 2 is included in the Week 2 Supplementary Data Descriptions download.

Organizationally, Big Marketing consists of three different branches, each with around 400 employees and its own web servers.

All Big Marketing workstations and servers sit behind a firewall, including the web servers that the company operates for their clients. The customers of Big Marketing's clients visit theses web servers regularly.

2. Network flow data.
Network flow data captures, to the extent feasible, the traffic moving across the network. Big Marketing captures network flow at the firewall, so transactions that go from Big Marketing to the internet, or come from the internet into Big Marketing, are captured.

In network flow data, a series of messages between two computers is combined into a single flow record. Records appear for each session where the handshake between the two computers is completed. While each flow record includes a source and destination IP, the designation of source and destination are not guaranteed to be correct. In a situation where the flow collector did not catch the initial transaction in a flow, and sees the response as the first transaction, the destination IP may be labeled as the source IP, and vice versa.

A detailed description of the network flow data is included in the Answer Sheet and Data Descriptions download.

3. Network health and status data.
A commercial network health monitoring program called Big Brother is installed on the network. Approximately every five minutes, each workstation and server sends a status update. The data format and further details are included with the Answer Sheet and Data Descriptions download.

4. Intrusion Protection System data.
For week 2, intrusion protection system (IPS) log data is also available. An IPS monitors and logs network activities. When it identifies apparently malicious activity, the IPS attempts to block or prevent the activity.

A detailed description of the IPS data is included in the Week 2 Supplementary Data Descriptions download.

5. Additional Questions.
As reflected in the netflow and Big Brother data, computer logs often do not contain the complete details needed to understand the event. As you notice events occur in Big Marketing networks, you may wish to consult other data sources to supplement your understanding. In this Mini-Challenge, you have a few opportunities to ask questions about items seen in the provided data. If the Big Marketing corporate office and/or the network analysts on your team have additional insight relevant to your question, you will receive an answer.

This method of expanding your analysis is optional and limited. You do not have to ask any questions. If you do choose to ask questions, you may ask at most five questions. Be aware that the phrasing and specificity of your questions is very important. If you ask a well-formed question, your analysts or the corporate office might be able to dig up some related information. However, it is also possible that no additional information is available. In spite of their best efforts to help with an investigation, additional information simply might not exist.

The procedure for asking questions is as follows:

1. Register your team by sending an email to VASTChalMC3@vacommunity.org that identifies your institution and the point of contact for your entry. You must complete this step before asking any questions.
2. To ask a question, send the question in an email to VASTChalMC3@vacommunity.org. Please include only one question per email. Responses will be sent within three business days.
3. After your quota of five questions has been answered, no further questions will be acknowledged.