A Framework for Effective Alert Visualization

Uday Banerjee
Jon Ramsey

SecureWorks
Visualization

• Visualization has always been used – but mostly from a reporting standpoint

• We need to start pushing it from the Reporting space to the Analytical space
Visualization

• Security departments/organizations deal with hundreds of thousands to millions(+) security alerts/messages a day from various devices:
  – IPS/IDS
  – Firewalls
  – AntiSpam / Antivirus devices, etc.

• Correlation is only so effective…

• Humans need to look at the outputs of the correlations, and should also be able to look at the larger picture to effectively analyze the situation
Visualization (contd.)
The case for Visualization

- Visualization is a very effective way to represent large volumes of information in a succinct manner.
- Allows one to look at the same data from multiple viewpoints.
- Allows one to look "around" the alerts that you are investigating to gain some additional perspective.
What makes a good visualization?

• Data driven display: we should be able to ‘slice and dice’ the data, bring related events into focus based on the data selected. E.g. select data by:
  – Protocol
  – IP Address
  – Timestamp
  – Asset Value
  – Port
  And have it bring into focus all related alerts.

• Multiple views into the same data: can elicit a different perspective
What makes a good visualization? (contd.)

• Data linkage across all views
• On-the-fly customization of views
• Drill down/Zoom out: allows to isolate a particular event-set or allows you to see the big picture
• Data suppression: allows to quickly eliminate data that is of no consequence to the analysis (e.g. UDP traffic when analyzing TCP flows)
• Statistical information: It is useful to know information on total or selected events (like totals, maximum values, unique values, etc.) to gain a perspective on the nature of the activity
What makes a good visualization? (contd.)

• Other desirable features:
  – Realtime visualizations
  – Interoperability with other systems (ticketing, reporting)
  – Easily accessible (via a web browser?)
Considerations for Effective Visualization

- Operator Considerations
- Infrastructural Considerations
- Design Considerations
- Data Considerations
Data Considerations

• Richer data sets make for better visualizations. We need to gather as much information around the event as possible
• Data should be normalized
• More visual correlation can be performed if there are a large number of data fields to work with. Some examples:
  – Device Interface > Tells you which interface the IDS/IPS alert was detected on > Tells us if the alert traffic was inbound or outbound
  – Action taken > was this alert blocked or allowed? > Different responses to alerts from IPS versus IDS
  – IP addresses > is the source IP on our ‘attacker’ watchlist?
  – Type of signatures tripped > specific attack or general scan
Infrastructural considerations

• Dedicated, capable database used exclusively for storing visualization data (allows for the flexibility to add/remove/modify content without affecting other production systems)

• Visualization tools should have access to other databases like Asset and Vulnerability databases so they can provide even more context
Operator Considerations

• If using color to key off on events, the ability of the operator to discern colors must be taken into consideration

• Screen real estate is *very* important

• Training
  – Using data from real scenarios
Design Considerations

• Design of the visualization is of utmost importance (layout, intuitiveness, features)

• The visualizations should be presented in such a way that inferences should quite literally, present themselves
Integration with our SIM Tool
Visualization: caveats

• Only becomes more effective as data grows larger
• May not be very suitable for quickly analyzing very small amounts of data
Some useful views

• Source IP vs Target IP vs Timestamp
• Source IP vs Target Port
• Source IP vs Alert Timestamp
• Dest Port vs Alert Timestamp
• Counts by (S_IP, T_IP, T_Port, etc.)
• Attacks vs Asset value vs Vulnerabilities
Demo