riverbed

Use Case

Automating Incident Response with Riverbed AppResponse

Security warnings, such as those from an intrusion detection system or a log-based alerting system, do not always immediately rise to the level of an incident.

In most cases these warnings are stored and remain available for later investigation if further sleuthing is warranted. Unfortunately, many security incidents take weeks or even months to unfold, with attacker "dwell time" growing over the last few decades. Riverbed® AppResponse APIs allow for automatic creation of relevant PCAP (short for packet capture) files that match any event of interest. This means that a security operator will have all the relevant packets available for any event when the time comes to dig deeper. Even when the event was months in the past.

Background

This global biopharmaceutical innovator deploys the entire Riverbed® Unified Network Performance Management (NPM) solution—full-fidelity flow monitoring, packet capture, and infrastructure monitoring—because they understand the adage: You cannot manage what you can't measure. They also support its corollary: You can't secure what you cannot see. And that's what we are exploring today.

Riverbed AppResponse packet capture and analysis provides valuable telemetry for both network and security operations teams. The network operations team might leverage its TCP metrics and Response Time Composition Chart to investigate reports of a slow application performance problem, while the security operations team can leverage packet data that AppResponse has stored to support a security investigation.

Incident Response Requires Packet Data

When deploying AppResponse, this biopharmaceutical customer's target goal is to retain 24 hours of packet data on any AppResponse appliance. The security team may need much longer history, especially when packets pertain to IDS/IPS/NDR detections but sometimes the packets of interest may have already aged out of the AppResponse capture buffer.

This situation is common to all packet capture solutions: The amount of time any packet capture solution can store packets is influenced by the volume of data being captured and the available packet storage on the appliance. While AppResponse provides granular control over what packets should be written to packet storage, the potential exists that the packets needed to support a performance problem or security investigation may not be available when they are needed. While adding more packet storage will help extend packet retention time, there will always be a limit to how much packet data it can retain. Riverbed professional services was able to provide a creative and successful solution to help the customer get the most from the available packet storage.

API Automates Packet Storage

Riverbed professional services provided the customer's security team with a two-step packet capture process for incident response:

1. Created an API that allows them to request packet captures for specified IPs, ports, and time ranges in an automated fashion based on events detected by their security tools. A request made to the API returns a list of AppResponse appliances that contain packets associated with the specified request.
2. A second API makes a subsequent request to any of the identified AppResponse appliances to retrieve the packets of interest. It then saves the packets to a secure FTP server for later analysis.

With the API framework in place, the customer was also able to build a web frontend for the security team and other stakeholders to request packet captures of specified IPs and port(s) for a specified start/end time. Once the request is scheduled and completed, the user receives an email message letting them know that their request is complete, and providing a secure link to where the requested packets are stored.

Stakeholder Benefits

This innovative solution improves the security team's agility and forensic recall capabilities by providing an automated process to preserve packet-based evidence associated with security events and the needed support for further security investigation. The solution extends the AppResponse ROI for the tools team by allowing them to satisfy additional stakeholders by extending packet retention time without necessarily having to invest in additional storage units.