

PQS for Network Security

Project description

INTRODUCTION

Modern network environments are protected by dozens of independent, uncoordinated security solutions, that all require individual inspection and viewing. In networks with hundreds of computers the sheer number of virus scanners, log files, personal firewalls, etc can be prohibitive, making it impossible for administrators to review all security information available, and link it with firewall logs, server logs, and intrusion detection systems. Using PQS we have developed a security system that brings together all sources of security information from anywhere in the network, and present it to the administrator in an organized and correlated fashion.

THE APPLICATION

PQS for Network Security offers an enterprise class network security monitoring application that gives a non-stop comprehensive view of the security status of your network, in addition to offering traditional security information management system functionality. Evidence of one attack may be scattered in many different places (think IDS, firewall logs, host and/or server logs). PQS for Network Security collects this information, correlates it, and presents it together to the user. Not only does this save significant amounts of time, it also allows a more in-depth and accurate view of the security status of your network, leading to better protection of your data.

The screenshot shows the PQS application interface. On the left, there's a 'Current' and 'Workbench' list with various IP addresses and status icons. The main area displays a 'Track summary' for an aggressor with IP 63.250.209.166, showing a threat score of 3179 and a hypothesis score of 0.5137. Below this, there's a log of events with columns for time, status, and message. At the bottom, there are controls for the PQS Server, including a port number (54322) and a 'Disconnect' button.

PQSEC TECHNOLOGY

Alert-based security (IDS/IPS) is quickly becoming a thing of the past. Today's attackers are getting smarter and more organized, carefully picking their targets with the goal of compromising revenue, stealing intellectual property, or defacing the public image. Integrated network situational awareness offers the ability to detect malicious behavior, rather than simply alert on signature matches.

The screenshot shows the C-track application interface. It features a 'File Server' section with 'PQS Server' and 'PQS Port' fields. Below this is a table of sensors with columns for IP, Port, Type, and Status. There are also sections for 'Hypothesis Scoring' and 'Publish Parameters' with various checkboxes and input fields. At the bottom, there's a log of events showing system status and connection attempts.

PROCESS QUERY SYSTEMS

A PQS is a generic correlation engine that puts the focus on the dynamics of an environment, instead of using traditional static methods. By describing how things change over time, a PQS is able to achieve previously unseen levels of detection and correlation in environments too complex for conventional techniques.

FUNCTIONAL SPECS

This PQS application has the following system requirements (for monitoring up to 1500 hosts):

- PQS platform (either PQSLite or C-TRACK)
- Pentium 4 or better
- SPARC III or better
- 512 MB RAM
- Java 1.4 or better
- MS Windows XP/2000, Linux 2.6, Solaris > 8

WOULD YOU LIKE TO KNOW MORE?

If you would like to learn more about this PQS application, or if you would like to use this functionality in your environment, please contact:

Vincent Berk
vberk@proquesys.com
16 Cavendish Court, Ste 211
Lebanon, NH 03766

