CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Lancope Stealth Watch NC and StealthWatch Xe Appliances containing StealthWatch V5.1.0 Software

Maintenance Report Number: CCEVS-VR-04-0064a

Date of Activity: 10 February 2006

References: Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004;

"Impact Analysis Report on changes to CC approved Lancope StealthWatch Appliance and StealthWatch + Therminator Applicance containing Version 3.3.0 – Build 4140 Software", version 1.0, 13 January 2006

Documentation Updated: Lancope StealthWatch developer evidence documents.

Assurance Continuity Maintenance Report:

The vendor for the StealthWatch Appliance, Lancope, Inc., submitted an Impact Analysis Report (IAR) to CCEVS for approval on 17 January 2006. The IAR is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version 1.0, February 2004. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

Security Relevant Changes:

The StealthWatch Appliance was changed to run atop SuSE Linux v9.1, instead of Red Hat Linux v9.0.

The System Data Collection security function was changed to allow receiving of network information from an external network infrastructure device (e.g., switch or router) via a Network Interface Card (NIC), in addition to receiving and monitoring raw network traffic.

The System Data Analysis and Reaction security function was updated to include additional security-relevant alarms and alerts that fall within the alarms categories identified in the certified version of the TOE:

- Data Deleted (Alarm) – StealthWatch has deleted (flow log) file(s), prior to their planned lifetime;
- UDP Worm Scan (Alarm) – a flow was detected exhibiting UDP Worm Scan characteristics;
- NAT IP (Alarm) – a host has been detected that is using a network address translated IP address;
- Alarm when log retention window is reduced.

Conclusion:

Because the TOE relies upon the underlying platform solely for time information, the change to the underlying platform was straightforward. The expanded services of the administration alarm interface is likely straightforward, as is the change to the data collection. All three of kinds of changes were tested by the developer and the testing documentation was correspondingly updated.

Consideration of the nature of the changes leads to the conclusion that they are best classified as minor changes and that certificate maintenance is the correct path to continuity of assurance. Therefore, CCEVS agrees that the assurance is maintained for this version of the product.