DATA SHEET

Iris Network Traffic Analyzer

INTEGRATED SECURITY AND THREAT MANAGEMENT SOLUTION

Iris Network Traffic Analyzer is designed to combine process and technology into a single effective system for network forensics.

Iris Network Traffic Analyzer empowers your security and operations teams by providing granular data monitoring and precise packet and session reconstruction capabilities. The solution is designed to combine process and technology into a single effective system for network forensics.

Today's organizations rely on the continuity and security of underlying IT systems at all times. This requirement is further amplified when you take into account the fact that most security or performance issues, whether due to malicious acts, user non-compliance or simple bandwidth misallocation, generally reside above your network in the applications being serviced by your infrastructure.

Iris Network Traffic Analyzer allows professional teams to quickly and easily examine the inner workings of a network. This highly sophisticated system supports the investigation into security and performance issues, decreasing the amount of detective work while enhancing the overall productivity of your security and performance monitoring systems.

SESSION RECONSTRUCTION

Most packet capture solutions and network sniffers only display raw packets and leave it to the user to decode and determine the potential problems they represent. Iris collects network traffic and reassembles it as its native session based format, enabling users to quickly and easily make business decisions based on the service it was providing. Iris users can present the actual text of an email, as well as any attachments, exactly as it was sent. It provides reconstruction of full HTML pages that an end user visited and reconstruction of cookies for entry into password-protected websites. Iris will even display bi-directional instant messaging communications allowing full session reconstruction as the end user sees it.

DATA CAPTURE

The Iris Traffic Capture Engine is designed as a service oriented architecture, permitting security professionals to gather forensic information while performing other tasks in parallel. Iris is designed to capture specific data

FAST FACTS

AVAILABLE AS SOFTWARE or bundled with the Retina 651 Security Management Appliance

PROVIDES INSTANT NETWORK data capture and the ability to decode traffic in real time

RECORDS AND REPLAYS traffic for a complete audit trail of suspicious network activity

HELPS IDENTIFY PERFORMANCE problems before they result in network downtime

COMPATIBLE WITH NETWORK adapters up to gigabit speeds

ADVANCED SEARCHING AND filtering for quick identification of desired datum

eEye Digital Security®

via filters based on a myriad of traffic metrics. This approach ensures that all targeted traffic is captured, regardless of whether the solution is run interactive or as a service. For capacity and service level agreement planning, Iris allows users to leverage traffic captured in one area of a network for use elsewhere, as well as for the monitoring of applications in development. Additionally, Iris allows for advanced functions such as keyword searching and protocol distribution.

STATISTICAL ANALYSIS

Iris provides a large variety of statistical measurements, supplying information on protocol distribution, top hosts, packet-size distribution and bandwidth usage. By regularly analyzing how systems and applications are being used, administrators can proactively identify and eliminate issues before they can result in downtime. Iris can also provide the proof required to drive the creation and enforcement of policies related to appropriate system and application usage.

- PROTOCOL DISTRIBUTION STATS: Reports network usage based on MAC, IP and IPX layer protocols.
- TOP HOST STATISTICS: Provides analysis of the IP layer traffic statistics collected for each host in real time and is ordered by the most “talkative” hosts.
- SIZE DISTRIBUTION STATISTICS: Displays the number of packets with sizes in six different ranges.
- BANDWIDTH USAGE: Charts the number of packets per second and bytes per second flowing across the network in real time.
- TRAFFIC REPORTS: Complete traffic data that can be viewed in a browser, saved, printed, or copied into another program.

DATA RECONSTRUCTION

Iris takes raw data packets and turns it into complete HTTP, SMTP, and POP3 sessions in their original format. The following are some of the protocols Iris reconstructs:

- OUTGOING AND INCOMING EMAIL MESSAGES: the text of the message is readable as well as the subject and recipient.
- WEB BROWSING SESSIONS: reconstruction of HTML pages in their original format.
- INSTANT MESSAGE SESSIONS: Iris will reconstruct all IM communications from both sides.

SYSTEM REQUIREMENTS

WINDOWS XP (32-BIT AND 64-BIT)
WINDOWS SERVER 2003 (32-BIT AND 64-BIT)
WINDOWS VISTA (32-BIT AND 64-BIT)
WINDOWS 7 (32-BIT AND 64-BIT)
WINDOWS SERVER 2008 (32-BIT AND 64-BIT)
WINDOWS SERVER 2008 R2
INTEL PENTIUM IV 2.0GHZ (OR COMPATIBLE)
512 MB OF RAM
40MB (SOFTWARE INSTALL)
20GB (CAPTURE STORAGE)
NETWORK NETWORK INTERFACE CARD (NIC) WITH TCP/IP ENABLED
MICROSOFT INTERNET EXPLORER 5.0 OR HIGHER

About eEye Digital Security

Since 1998, eEye Digital Security has made vulnerability management simpler, less expensive, and more effective by providing the only unified vulnerability and compliance management solution that integrates assessment, mitigation, and protection into a complete offering. Consistently the first to uncover critical vulnerabilities and prevent their exploit, eEye leverages its world-renowned research and development to strategically secure customer assets. Thousands of mid-to-large size organizations, including some of the most complex IT environments in the world, rely on eEye solutions to protect against the latest known, unknown, and zero-day vulnerabilities.

See more at www.eeye.com

CONTACT INFORMATION

UNITED STATES
1.866.282.8276

GERMANY
+49 (0) 8031 2227 432

UNITED KINGDOM
+44 (0) 20 8432 3490

NORTH AMERICA SALES
sales@eeye.com

INTERNATIONAL SALES
sales.eu@eeye.com

www.eEye.com

111 THEORY, SUITE 250 | IRVINE, CALIFORNIA 92617

© 2011 eEye Digital Security. All Rights Reserved.