



Intrusion Detection

Intelligent Event Correlation IEC2

Overview

RandomStorm's enterprise threat management environment has been designed by security professionals that have extensive direct experience of the commercial pressures that network managers have to face. One of the most challenging aspects of this critical corporate role is recognising which of the vulnerabilities represents the most immediate threat and any that, albeit serious, can be given lower priority attention.

Intelligent Event Correlation

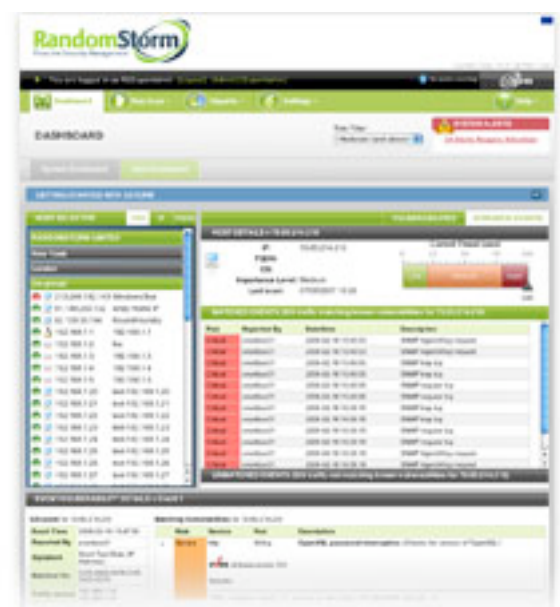
RandomStorm's iStorm technology is an integrated network vulnerability and event correlation engine based around a unified graphical management dashboard. Using the technology, network managers are able to schedule routine scans of the whole network or just critical hosts as often as is necessary, providing a detailed analysis and threat assessment of any vulnerability that is discovered. Uniquely the system also includes a range of plug-in options to enable security intelligence to be harvested and correlated from different vendor technologies installed in the network, including IDS and firewall information, identifying any that need immediate action and significantly reducing the number of false positives.

RandomStorm combines its understanding of asset vulnerabilities with real time intrusion detection alerts, dramatically reducing the amount of misleading information normally associated with an IDS deployment. By analysing the attack and filtering the events that have no impact RandomStorm IEC2 frees up IT managers' time and budgets to focus on genuine risks to the enterprise.

Randomstorm IEC2 is an open and extensible event correlation gateway that allows IT managers to leverage existing investment in IDS and end-point security technologies. Based on a highly graphical and intuitive management dashboard the system combines detailed vulnerability information of the network assets with real-time threat data such as spyware, port scans and Trojans, alerting network managers to any real and present dangers in time to take remedial action to avoid an event escalating into a business critical incident.

Increased Productivity

RandomStorm addresses the fundamental pain points felt by all network security managers faced with the challenge of maintaining security defence at the highest level within a finite budget and limited resources. With new threats and vulnerabilities appearing on a daily basis it is a daunting task to keep on top of a complex network topology that can include hundreds of individual "at risk" devices. IEC2 enables the process to be automated and streamlined, reducing the risk of human error and obtaining maximum RoI for the business.



RandomStorm Event Correlation dashboard