

Tableau Thwarts Network Security Threat

Stanford University Identifies and Arrests Hacker Intrusion with Visual Analysis

Company Profile

Founded in 1891, Stanford University is one of the most respected research and academic institutions in the world.

Customer Case Description

The Computer Graphics laboratory is designed for teaching and research. The infrastructure of the lab is maintained by active collaboration of the faculty, staff, and students.

In July 2004, the laboratory manager received an e-mail from the university's networking department complaining about a rogue FTP server running within the stanford.edu domain. That day the machine had produced very high traffic volumes to offcampus locations and the manager was asked to investigate.

The data used in the analysis consisted of Cisco NetFlow records from a Stanford router. A network flow is defined as a unidirectional sequence of packets between a given source and destination endpoints. Network flows are highly granular; flow endpoints include a time-stamped summary of source, destination, protocol, and number of packets and bytes. Each source or destination consists of an IP address and a port.

The primary challenge was to find and implement an analysis application that supported this type of investigation. In particular, the application needed to (1) support Microsoft SQL Server, (2) be able to quickly sift through millions of records of data, and (3) be able to manipulate and display many dimensions of the data simultaneously.

The Solution

Stanford University selected Tableau Professional.

The visual analysis features of Tableau enabled Stanford to "see" this complex data from many perspectives and focus on the important relationships and key insights. Tableau's advanced filtering functionality and its ability to quickly iterate through multiple ad hoc queries and displays made it uniquely suited for this investigation.

For More Information About This Case

Contact: visualanalysis@tableausoftware.com or call (206) 633-3400 x1



"Tableau's visual layout and filtering capabilities allow us to reduce datasets of millions of network connection records to understandable views, and its flexible output options enable us to visually analyze hundreds of thousands of them as we search for the source of an intrusion."

John Gerth, Manager, Computer Graphics Lab