OVERVIEW

The Information Technology Agency (ITA) manages the IT infrastructure and its security for the City of Los Angeles - part of the greater Los Angeles Metro area with a population of 13M. As employees of the City of Los Angeles, ITA ensures the business of government is efficient by providing an information technology infrastructure and systems that are reliable, long-term, financially viable and secure. It continuously strives to improve the dissemination of public service information through the expanded use of communications, computing technology and effective telecommunications oversight.

ITA provides technical support services to City departments with application design and development, post-implementation support, problem analysis, technical consulting, project management and contractor monitoring. It is also responsible for the City’s E-Government and Web services, including the website and application design and development, publishing of City web development standards, webmaster support, client consultation and training and maintenance of Citywide Internet and Intranet Web sites. Although the agency has 500 people, only a few are directly tasked with securing the City’s systems.

CHALLENGES

ITA needed to secure the city’s computer infrastructure - a large network with several thousand routers and switches and over 500 application and web servers and mainframes. This incorporates its financial systems, LAPD (police department), critical systems for all departments. As it includes ten websites that process credit card payments, the agency also need to ensure its systems were compliant with the PCI Data Security Standard (PCI-DSS).

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. A comprehensive standard, it is intended to help organizations proactively

“We deployed a leading SIEM for security management, but because of budget constraints, we couldn’t cover all the devices we needed to monitor…. AlienVault’s bundled VA and IDS capabilities save the city money that would otherwise be spent on additional products.”

Brian Cao, System Programmer, City of Los Angeles
protect customer account data. For ITA, this meant it had to collect and store system logs, between 10,000-15,000 events per second, from all devices that process credit card information, including its firewalls and intrusion prevention systems.

As with all governmental agencies its budget was minimal, to non-existent, and manpower was exceptionally scarce!

the **SOLUTION**

ITA had already purchased a product from a leading SIEM vendor. However, it was finding it very expensive to maintain, and that SIEM alone was not enough. Modern threats require a large number of security controls working together to effectively identify attacks and appropriately react. For ITA, it couldn’t afford the additional investment required to scale up the solution to secure its entire complex network. A further frustration for ITA was that customizing the solution, to collect data from its in-house systems, was proving impossible.

Having heard about OSSIM by AlienVault, ITA started to use the open source tool to see just what it could do. Suitably impressed, it quickly converted to the AlienVault Unified Security Management (USM) Platform.

“The AlienVault feed subscription provides a lot of reports and more effective correlation rules out of the box …which is important because we don’t have a lot of people to help us.”

Brian Cao, System Programmer, City of Los Angeles

the **BENEFIT**

The AlienVault USM Platform has the best open-source security controls built in. It brings together five critical security capabilities – asset discovery, vulnerability assessment, threat detection, behavioral monitoring, and security intelligence – to provide a quick and easy way to protect the enterprise with minimal integration and deployment overhead.

Simple to deploy, ITA found as soon as it was plugged in the platform, the solution started discovering its assets to help identify the critical systems that were deployed, and performed vulnerability assessments to identify any potential weaknesses in those systems. AlienVault USM Platform is capable of detecting threats using network, host, and wireless intrusion detection, and monitors the behavior of the systems to identify deviations that could indicate a breach.

This combination of AlienVault’s simplified deployment model and built-in security controls gave ITA the immediate visibility that, until then, it had only dreamed of. ITA was able to customize the AlienVault plug-ins itself and build connectors to collect data from its legacy and best of breed anti-virus, intrusion detection and intrusion prevention systems. With the AlienVault feed subscription ITA is able to utilize a lot of reports and more effective correlation rules out of the box. Additionally it is able to log its sizeable quantity of events, and easily store them for as long as necessary. Finally, with the AlienVault Compliance Management solution, ITA can meet all its regulatory requirements easily, and affordably.

The icing on the cake for ITA is that it could now manage and secure its extensive infrastructure, with very limited staff, and save money that otherwise would have been spent procuring the additional products needed to compliment its previous SIEM solution.

AlienVault, U.S.
1901 S. Bascom Ave, 520
Campbell, CA
95008

t: +1 408.465.9989
f: +1 408.550.2726

AlienVault, Europe
C/Cronos 63
Planta 2a, Oficina 6
CP: 28037 Madrid, Spain

t: +34 91 515.1344
f: +34 91 413.5968

AlienVault, U.K.
Davidson House
Forbury Square
Reading, RG1 3 EU

t: +44 (0) 118 900.1770
f: +44 (0) 118 900.7818