Splunk for F5 Application Security Manager

Splunk provides Application Security Manager users with advanced search and reporting capabilities

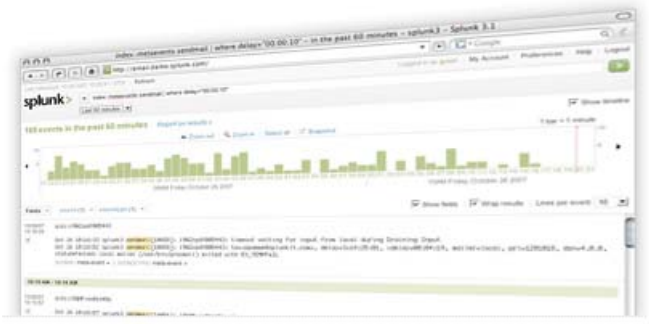
Some of the most serious network security threats come from attacks that target vulnerabilities in enterprise applications. These attacks ignore conventional firewalls and intrusion-detection and prevention systems, and they are often difficult and costly to prevent.

BIG-IP Application Security Manager (ASM) delivers comprehensive protection for Web applications and operational infrastructure. BIG-IP ASM employs an auto-adaptive approach to application delivery security, where the security policy is automatically updated based on observed traffic patterns. This simplified approach to configuration makes implementation and maintenance easier, reducing the overall total cost of ownership.

In the course of protecting web applications, ASM produces detailed log files about each transaction it filters. While ASM comes packaged with detailed reporting capabilities already, some customers may need to perform even more advanced searches, reporting and alerting on the data using a specially-designed analysis tool. Incident response, threat analysis, event correlation from multiple network devices or compliance audits are common examples of activities that can require advanced investigation. For users with these advanced needs, F5 has partnered with Splunk to offer a solution specifically tailored to ASM.

What is Splunk?

Splunk is an IT information search solution that indexes data and enables users to analyze, alert and report on all their IT data from every application, server and device; all in one place. It enables you to find and fix problems, investigate security incidents before attackers cover their tracks and generate compliance reports quickly and easily.



Splunk continuously indexes all your IT data by time so you can see change in action. And it dynamically interprets the data when you perform a search, eliminating the need to keep up with ever changing data formats. It doesn't require special agents, adapters or parsers for specific data formats and you get the correlation you need without writing lots of elaborate rules.

Splunk can integrate with your existing enterprise management, security and compliance tools right out of the box. The Splunk toolbar makes it simple to launch searches from any web-based application and Splunk alerts can be sent to any of your existing consoles. It can even index the data already collected by your existing management tools to extend the life of your investments.

How the ASM Application for Splunk Works

F5 and Splunk have partnered together to develop a specific ASM reporting and analysis template that can be installed as an add-on "application" to the core Splunk application. Security experts at F5 and Splunk designed the ASM plug-in to specifically meet the needs of advanced ASM users who are seeking detailed information. Examples of these reports are listed below, and additional reports can be easily and quickly built within the Splunk administrator console. Some of the reports included in the ASM application for Splunk are:

- Top violations
- Top violations by protocol (HTTP, FTP, SMTP)
- Top HTTP violations by web application
- Top attackers
- Top attackers by protocol (HTTP, FTP, SMTP)
- Top web applications attacked, alerted or blocked
- Top web applications alerted by IP address
- Attacks by location
- Top response codes by web application
- Top alerted or blocked web application requests by time period
- Web application requests by method
- Custom ASM forensics filtering & search

In addition to producing an add-on Splunk application for ASM, F5 and Splunk have also developed one for F5's secure remote access solution, the FirePass controller.

Splunk also provides additional add-on applications to cover compliance reporting such as PCI. These applications help customers meet the requirements set forth in the latest PCI v1.2 by collecting and reporting on other devices within an organizations infrastructure. The PCI application from Splunk includes over 60 reports and saved searches that help customers meet PCI auditing requirements.

About F5 and Splunk:

F5 and Splunk have partnered to deliver an advanced security reporting and analysis tool to assist ASM users. This brings even more value to users of F5's Application Security Management solution, and enables them to meet the complex needs of incident responses, threat analyses or compliance audits.

The Splunk product can be purchased directly from Splunk, and the ASM application is available for free download.

For more information on Splunk, see www.splunk.com

For more information on ASM, see www.f5.com

For more information on the ASM application for Splunk, see www.splunk.com/partners/f5

F5 Networks, Inc.
Corporate Headquarters

401 Elliott Avenue West
Seattle, WA 98119
(206) 272-5555 Voice
(888) 88BIGIP Toll-free
(206) 272-5556 Fax
www.f5.com/info@f5.com

F5 Networks
Asia-Pacific

+65-6533-6103 Voice
+65-6533-6106 Fax
info.asia@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa

+44 (0) 1932 582 000 Voice
+44 (0) 1932 582 001 Fax
emeainfo@f5.com

F5 Networks
Japan K.K.

+81-3-5114-3200 Voice
+81-3-5114-3201 Fax
info@f5networks.co.jp