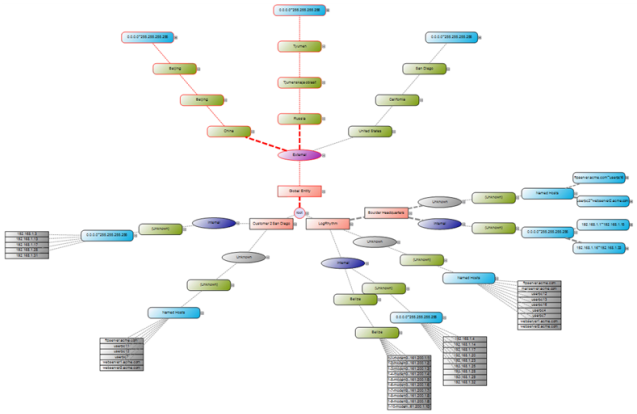
LOGRHYTHM LABS EMBEDDED EXPERTISE

Security Analytics Suite - Web Application Defense

LogRhythm Labs

The use of web applications is integral to meeting many business-level objectives. Web applications connect end users to organizations, improving accessibility to data which facilitates corroboration and increases efficiency. While web applications provide distinct value, their network connectivity and access to sensitive data such as user credentials, financial and payment data make them prime targets for motivated attackers looking to gain access to the corporate network.



Web Application Defense - Investigation on Attacking IPs

LogRhythm Labs' dedicated team of security experts performs advanced research to recognize how LogRhythm's Security Intelligence Platform can expose attack behavioral patterns against web servers and applications. Research from the Labs team is continually embedded in the Web Application Defense Security Analytics Suite via bi-weekly updates to help organizations strengthen network and web security.

The Web Application Defense Security Analytics Suite is designed to analyze web server logs and other related data sources with a focus to detect, identify, and prevent threats and breaches. When malicious web behavior is identified, the associated IP address is automatically added to a watch list of attacking IPs. Using LogRhythm's SmartResponse™, the watch list can also be leveraged to create a blacklist that enables your network infrastructure to block any further access attempts. The suite delivers meaningful alerts and automated remediation to detect and prevent attacks targeting web servers.

Web Application Defense in Action

LogRhythm's comprehensive collection capabilities combined with real-time advanced correlation enable organizations to monitor web applications for signs of suspicious activity. The Web Application Defense Security Analytics Suite helps organizations detect the following scenarios:

Website Defacement: Website defacement is not only devastating for corporate brand image, it can also help facilitate the transfer of malicious code to end users attempting to access the site. The Web Application Defense Suite builds a behavioral baseline of normal website activity and triggers an alarm whenever a deviation from the norm is observed. This early indicator can alert IT and security analysts to quickly investigate the root cause and take steps necessary to secure the site and mitigate any impact on end users.

SQL Injections: Organizations using web applications need to be able to detect application layer attacks such as SQL Injections that attempt to distort the back-end code to gain illegitimate access to high-value data. The Web Application Defense Suite references a list of attack types generated by security hacking tools and an AI Engine rule analyzes web server logs to detect the introduction of these malicious strings. A Smart**Response**™ plugin can automatically add the IP address to a watch list or firewall access control list.

Cross site scripting: Dynamic web applications that allow user input deliver a lot of value to end users, but their interactive capabilities make them susceptible to cross-site scripting attacks. The Web Application Defense Suite provides an AI Engine rule that looks for common URL-encoded script tags, indicating a reflected or stored cross-site scripting attack. When this type of behavior is detected, an alarm is triggered enabling IT and security teams to isolate the infected website.

LogRhythm's Web Application Defense Security Analytics Suite provides out-of-the-box Lists, AI Engine Rules, Investigations/Layouts and Smart**Response**™ plug-ins that enable organizations to effectively detect suspicious web activity. The suite is constantly updated, based on ongoing research from LogRhythm Labs. Below is a sample of the content provided in the suite.

Lists

Suspicious URL Characters	List of URL characters generated by security/hacking tools
Malicious User Agent Strings	List of user agent strings used by security/hacking tools
Attacking IPs	Dynamic list populated by Smart**Response**™ plugins in response to suspicious IP addresses detected by AI Engine rules
Bad Bot User Agent Strings	List of User Agent strings that exhibit malicious behavior such as email harvesting or spam referral bots

AI Engine Rules

Suspicious URL Characters (Internal and External)	Monitors web server logs for the presence of malicious characters in the URL string requests coming from external or internal hosts
Malicious User Agent (Internal and External)	Monitors web server logs for the presence of user agent strings used by hacking/security research tools from external and internal hosts.
Bad Botnet User Agent (Internal and External)	Monitors web server logs for the presence of user agent strings used by known bad actors or spam referral bots.

Investigations / Layouts

Attacking IPs	Investigations and Layouts will filter down on the attacking IPs list generated by the Web Application Defense Module

Smart**Response**™

Add Item to List	Automatically adds offending IP addresses to the Attack IPs list

Deployment

The Web Application Defense Security Analytics Suite can be deployed in environments with multiple operating systems including various Linux, Windows, and Solaris distributions. By design, this module can be used in combination with industry standard Intrusion Detection Systems and Web Application Firewalls to increase the amount of information available for real-time correlation and event recognition. Implementation is as simple as enabling the module and subsequent alerts from within the console.