

LOGSIGN AND PALO ALTO NETWORKS FOR AUTOMATED RESPONSE

Benefits

The Palo Alto Networks Technology Partner Program includes a select group of partners that deliver solutions or products that interoperate with the next-generation firewall.

Logsign and Palo Alto Networks for integrated enterprise security enable:

- Automated Responses.
- Finding Anomaly to Link.
- Fast Response Times.
- Real-time Detection

Logsign and Palo Alto Networks have partnered to deliver heightened awareness to enterprises. Integrated seamlessly, Palo Alto Networks next-generation firewalls send logs into Logsign via Syslog in a rich context including all user and application activities.

In addition to detecting any anomalies on a single or multiple IP addresses, this seamless integration allows Logsign to take automated actions on firewalls.

The Palo Alto Networks and Logsign Integration Provides:

Logsign reads the pre-defined rules and rule fields such as source, destination, action and many others on Palo Alto Networks firewalls. If there is a match between the detected IP address and the rules, Logsign adds that IP address to the dynamic IP list. By the way acts automatically as it is defined in that rule.

Consequently, Logsign responses automatically on behalf of the IT teams by automatically modifying Dynamic IP lists, blocking IP addresses, adding new ones or deleting that ones from the list in regard to the rules that are predefined on firewalls.

About Logsign

Logsign is a full feature, all-in-one SIEM solution. It unifies Log Management, Security Analytics and Compliance. Built on the NoSQL infrastructure it relies on the principle that centralizing log data, analyzing in real-time and providing actionable insights is critical for business continuity. Logsign delivers a great value and visibility for organizations at detecting threats and vulnerabilities in real time. Beyond correlation, Logsign automates prevention actions with active, built-in responses and meets requirements for international compliance processes.

Logsign is easy to deploy within a week. The user-friendly platform is backed up by a diligent technical support team providing customers a reliable solution for an affordable price in today's SIEM market. Since 2012 hundreds of SMBs and more than 400 local and global enterprises have deployed Logsign. Our community of satisfied customers is growing day by day as we continue with our focus on delivering added value for our customers.

About Palo Alto Networks

As the next-generation security company, we are leading a new era in cybersecurity by safely enabling all applications and preventing advanced threats from achieving their objectives for thousands of organizations around the world. We are the fastest growing security company in the market because of our deep expertise, commitment to innovation, and game-changing security platform focused on bringing an end to the era of breaches by uniquely integrating our Next-Generation Firewall, Advanced Endpoint Protection, and Threat Intelligence Cloud.

Because these capabilities are natively built into our platform and designed to deliver highly automated preventative measures against cyber threats, we ensure superior security to legacy point technologies such as stateful inspection firewalls, UTMs, or endpoint security products. With our platform, organizations can confidently pursue a digital-first strategy as they implement key technology initiatives within the cloud and increasingly mobile networks, while maintaining complete visibility and control, to protect their most valued data assets and critical control systems

Use case #1

Detect and Respond to Additional Anomalies

Challenge:

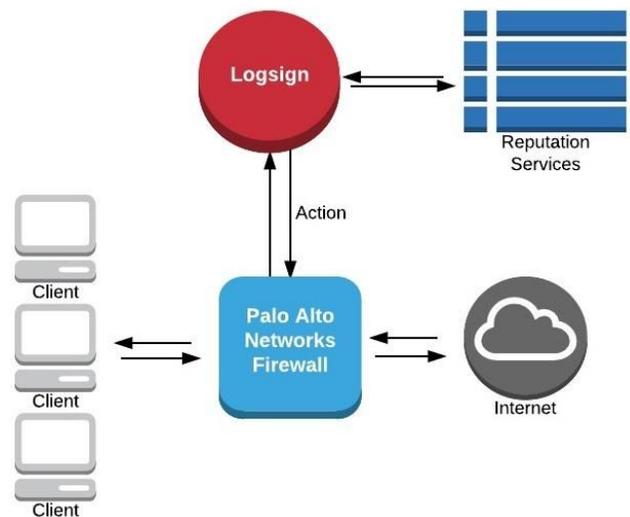
SIEM solutions need to work with the trusted reputation services to question the data rapidly. Once the response is taken, it should be correlated with all the data. In addition to that dashboards, reports and alerts should be generated.

Solution:

Logsign analyzes, data that imported from various trusted reputation services with Palo Alto data.

Response:

Logsign enables a rule to block and triggers Palo Alto firewall to respond automatically when there is an unwanted access from an IP address on that IP reputation list is detected.



4401 Great America Parkway
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2016 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <http://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.