Splunk Adaptive Operations Framework
Technology Partner FAQ

Last updated 09/2018

STRATEGIC OVERVIEW

What is the Splunk Adaptive Operations Framework (AOF)?

- The Splunk Adaptive Operations Framework (AOF) is an evolution of the Adaptive Response Initiative to include the robust Phantom community. By bringing together the industry's largest ecosystem of innovative security vendors, the Splunk AOF provides the necessary integrations to ingest data from anywhere, drive collaborative decisions with rich analytics, and take orchestrated action across a range of technologies in the security operations center (SOC).

How does AOF address market needs?

- Today's security customers are facing two main challenges: 1. an industry-wide skills shortage and 2. the struggle of having to use an average of more than 70 tools and technologies in their environments. When combined together, they often cause difficulty when it comes to gaining visibility or driving coordinated actions across disparate sources. As such, security vendors are looking to collaborate and help bridge the gap of managing multiple security domains.

  Meanwhile, customers are also driving the demand for integrated solutions with their SOC and a growing number of our customers are incorporating Splunk's leading SIEM (Security Information and Event Management) and SOAR (Security Orchestration Automation and Response) technologies into the center of their security operations. The result? Security vendors that offer out-of-the-box integrations with Splunk can benefit from reduced friction in the sales cycle, increased customer adoption, improved customer success and satisfaction.

I'm already a participating partner in the Splunk ARI and/or the Phantom Community - what's next for me?

- Let's do more together! The Splunk AOF is flexible and addresses your needs and interests as a partner:
  - Interested in aiding customers in getting their data into Splunk and gaining answers to address their security challenges? Great!
  - Interested in helping customers make decisions and take action based on bi-directional integrations you've built? Awesome!
  - (And for those who are more adventurous…) interested in developing integrations to help customers perform orchestrated actions and automated workflows across their technologies in their SOC? Excellent!

Splunk Adaptive Operations Framework
Technology Partner FAQ

Last updated 09/2018

Splunk's leading technologies are widely adopted and partners should continue to build integrations with Splunk so that you have the opportunity to expand customer use and adoption of your products - growing pipeline and revenue.

How does ARI/AOF impact my customers?

- Customers have successfully implemented similar capabilities for many years, and Splunk technology and partnerships are foundational to accomplish the mission of the initiative. Here are a few customers who are using Splunk AOF capabilities:
    - Aflac is using ThreatConnect Adaptive Response actions to execute actions in Splunk Enterprise Security (see blog for quote)
    - Blackstone is automating malware investigation with Splunk Phantom
    - Symantec (public at .conf)

GUIDELINES FOR DEVELOPMENT

How can I build on the Splunk AOF?

- Splunk AOF ecosystem partners can develop integrations - in the form of Splunk apps and add-ons - that can be used across Splunk solutions to aid customers in unlocking answers out of their data:

    Splunk Enterprise | *Splunk Cloud* | *Splunk Enterprise Security* | *Splunk Phantom* | *Splunk User Behavior Analytics*

- Splunk AOF ecosystem partners can develop bi-directional integrations within the Adaptive Response Framework in Splunk Enterprise Security as Adaptive Response actions to aid customers in driving collaborative decisions and actions supported by rich analytics
- Splunk AOF ecosystem partners can develop Splunk Phantom Apps and Playbooks to aid customers in driving comprehensive, flexible, and well-coordinated integrations to perform orchestrated actions and automated workflows across their technologies

Does this change anything with the development and integrations we have built already?

- All existing integrations with Splunk and Phantom will continue to be supported as they are today.

Are there any resources to follow in order to build to the Splunk AOF?

- We have resources available, with more coming soon. You can get started here:
    - Splunk AOF Home Page: http://splunk.com/aof
    - Splunk Developer Resources: http://dev.splunk.com
    - Phantom Community: https://www.phantom.us/community/

- Splunk AOF Solution Guide: https://www.splunk.com/pdfs/solution-guides/splunk-adaptive-operations-framework.pdf

How can I join?

- The Splunk AOF offers partners multiple ways to strengthen their alliance with Splunk through different points of integration, as well as the opportunity to reach more customers. All partners not currently participating in the initiative are encouraged to join. For more information, please visit our Technology Partner Program application or email adaptive-operations@splunk.com

For further information on how to join or how to build out integrations, please contact the Splunk team directly at adaptive-operations@splunk.com.

Additional Resources

- Web Page: https://splunk.com/aof
- Blog Post (public after .conf)