splunk>

PROFESSIONAL SERVICES

Splunk UBA Implementation Success

Get your User Behavior Analytics project going quickly

Machine Learning, Anomaly Detection, and User Behavior Analysis (UBA) projects are complex, technically advanced, and require a highly-trained team to help customers successfully implement a program that will meet their needs.

Splunk User Behavior Analytics (UBA) is a machine learning-powered solution that delivers the answers you need to find unknown threats and anomalous behavior across users, endpoint devices and applications. It not only focuses on external attacks but also the insider threat. Its machine learning algorithms produce actionable results with risk ratings and supporting evidence that augment security operation center (SOC) analysts' existing techniques for faster action.

Three Sizes to Meet Your Needs

Every customer is different, so we have built three different sizes to provide flexibility to different needs. Each of our offerings will bring you a full Splunk UBA installation, including integration with Splunk ES if applicable.

Base Offering

Spend time with a Splunk Solutions Architect to discover requirements and customize the project plan.

A Splunk Accredited Consultant then executes the plan, installing a fresh copy of Splunk UBA. They will ensure all UBA required data sources are coming in to UBA and are normalized correctly.

Once data is in place, the Consultant will enable and tune Splunk's use cases recommended for UBA. There is project coordination and success tracking along the whole project by the Splunk Delivery Manager.

It is expected that if you are looking to monitor Users and account behavior, access to Active Directory will be required.

Standard Offering

Receive everything in the Base Offering, then delve deeper into custom use cases. Receive further onsite training for both the Admin and Hunter/Analyst. New additional data sources can be added to support defined use cases.

Premium Offering

Receive everything in the Standard Offering. In addition, the UBA team will provide a bi-annual optimization and upgrade service, a Professional Services workshop, and an onsite Professional Services Associate Consultant to operate the UBA system while you grows your in-house UBA team.

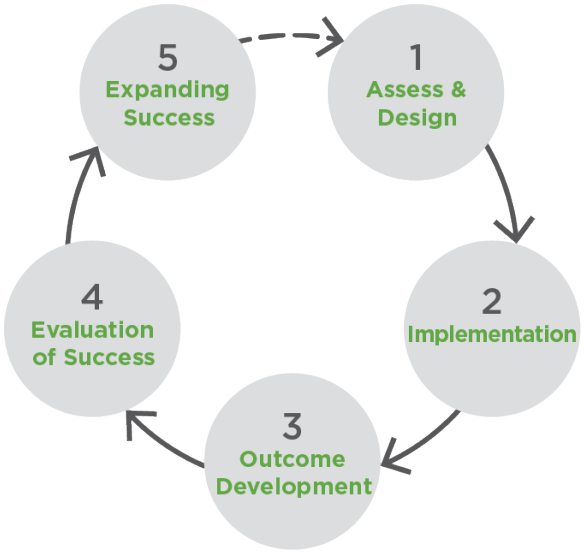
Data Sources Required

As this is a prescriptive offering, the following data sources will be required to receive all outcomes:

- Firewall
- Proxy
- VPN
- Windows Security Event Logs
- DNS
- DHCP

Splunk Success Methodology

Leveraging the experience of thousands of Splunk deployments, the Splunk success methodology will quickly bring you to your desired outcome.



Outcomes

Below are some of the types of tasks that the Splunk Professional Services team can assist you with.

Category	Outcome	Base	Standard	Premium
Understanding and Architecting	Workshop to Determine Success Criteria, Challenges, Opportunities, and Customize Project Plan	✔	✔	✔
	Install UBA per Guidelines	Multi-Tier	Redundant	Redundant
	Onboard Data to UBA	Limited to 6 Data Sources (prev. page)	+ 3 Data Sources	+3 Data Sources
	Workshop to identify Future Customer Use Cases			✔
Security Visibility	Activation of 50+ Anomaly Detection Use Cases	✔	✔	✔
	Tuning of Use Cases	✔	✔	✔
	Enhanced Customer Use Case Tuning			✔
Enhance Training and Operations	Enhanced Training		✔	✔
	Onsite Operations Assistance			✔
	Adding Additional Data Sources		✔	✔
	PS Workshop			✔
	Bi Annual upgrade, health check			✔

Target Customer Attributes

The Splunk Professional Services UBA Implementation Success Offering is designed for customers looking to enhance their Security posture with deeper Anomaly Detection Analytics.

Splunk Professional Services

Our services are backed by Splunk Accredited Consultants, Solutions Architects, and Delivery Managers. They leverage Splunk best practices and experience from thousands of Splunk deployments.

We only exist to get customers to valuable outcomes with their machine data – faster than they could on their own.