splunk> turn data into doing

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.

Data Sources Required

As this is a prescriptive offering, the following data sources will be required to receive the basic set of analytics delivered by the Models and ML in UBA.:

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

Offering Details

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

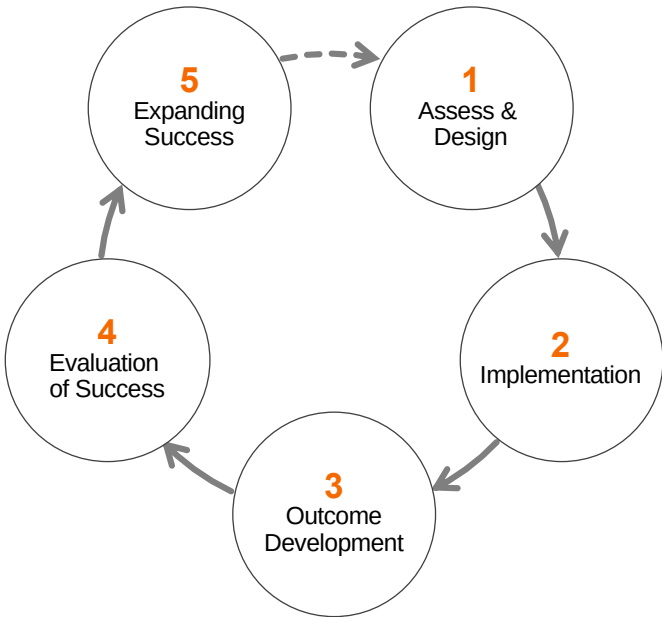
A Splunk Accredited Consultant then executes the plan, installing a fresh copy of Splunk UBA. They will ensure all UBA required data sources are coming in to UBA and are normalized correctly.

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 Project Manager.

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

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	Offering
Understanding and Architecting	Workshop to Determine Success Criteria, Challenges, Opportunities, and Customize Project Plan	✔
	Install UBA per Guidelines	✔
	Onboard Data to UBA	Minimum 6 data sources
Security Visibility	Activation of 100+ Anomaly Detection Use Cases	✔
	Tuning of Use Cases	✔
	Enhanced Customer Use Case Tuning	✔
Training and Operations	Onsite Training	✔

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.