# Splunk UBA Implementation Success

Splunk User Behavior Analytics Adoption Acceleration

**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.

## Accelerate Your Success

The Splunk UBA Success offering is designed to get you quickly and comprehensively up and running with Splunk User Behavior Analytics. The offering is designed to apply Splunk best practices, provide recommendations for improvement, and accelerate your journey to realize the full capabilities of Splunk User Behavior Analytics. 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.

## Offering Details

This Professional Services offering is for Splunk UBA only. Our Experts may perform the following activities for the Standard offering of Splunk UBA:

- **Implementation Planning Workshop**: Spend time with a Splunk Solutions Architect to discover requirements and customize a project plan that will define the work to be performed for the duration of the project. There is project coordination and success tracking by the Splunk Project Manager.
- **Configuration Services**: A Splunk Accredited Consultant will utilize best practices for installing Splunk UBA while executing the project plan. They will ensure all UBA required data sources are coming into UBA and are normalized correctly.
- **Use Case Review Sessions**: Once data is in place for the recommended baseline period and use cases are enabled, the Consultant will operationalize and tune Splunk UBA use cases.
- **Knowledge Transfer Sessions**: Professional Services will conduct sessions to demonstrate the implementation and document administrative items. Best practices will be communicated and shared on the overall administration of the application.

## 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 machine learning in UBA:

- **Account Data** (HR Data or Active Directory)
- **Asset Inventory**
- **DHCP**
- **Firewall**
- **Proxy**
- **VPN**
- **Windows Security Event Logs**

## Additional Data Sources

In addition to the required data sources, the following data sources unlock additional detections for a variety of use cases in Splunk UBA:

- **Authentication**
- **Badge Access**
- **Cloud Data**
- **DLP**
- **DNS**
- **Email**
- **Endpoint**
- **External Alarm**
- **IDS/IPS**
- **Host AV**

## 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 7 data sources |
| | Provide Options for High Availability or Disaster Recovery Requirements | ✓ |
| Security Visibility | Activation of 100+ Anomaly Detection Use Cases | ✓ |
| | Tuning of Use Cases | ✓ |
| | Enhanced Customer Use Case Tuning | ✓ |
| Knowledge Transfer | Conduct Knowledge Transfer Sessions to Review Best Practices | ✓ |
| | Solution Overview and Customization Assistance | ✓ |

## Target Customer Attributes

The Splunk Professional Services UBA Implementation Success offering is designed for customers looking to incorporate a solution using machine learning and anomaly detection analytics in their security operations center to prevent, detect and respond to cyber attackers in today's security landscape.

## Splunk Professional Services

We are here to help customers get the most out of our products. Our services are backed by Splunk experts, who provide consistent and quality service delivery, architecture guidance, training and ongoing support. Take your Splunk environment to the next level and achieve continual optimization, enhanced processes and active collaboration.