

UBA In depth

With a proven track record of success, our team of experts has perfected the process of making your organization take the next step into fighting internal threats by deploying UBA (User Behavior Analytics).





Whether is guidance into planning, creating use-cases or extending UBA through your organization, as trusted advisors, Professional Services is here to help you all the way.

Top UBA deployment concerns:

Planning for an effective QRadar User-Behavior Analytics deployment can be overwhelming. Here are the **TOP** concerns customers share:

- **Readiness** of a security program that outlines effective **use-cases** to be applied into the organization.
- **Gaps** of current QRadar deployment to be **addressed** before deploying UBA.
- **Strategy** for rolling out User-behavior analytics **enterprise** wide.
- Not enough **prepared resources** to handle **incidents** detected by User-behavior analytics.

Innovative Solutions:

-  Capturing **voice of the customer** feedback, through expertly guided workshops, understanding concerns (determining what really matters) is a cornerstone for success.
-  Informed decision making during **solution selection**, i.e. assess deployment options, identifying solution design accelerators, and solidifying associated timelines.
-  Expert advisor will **greatly reduce risk** of loosing existing customization investments, as well as offset resource demands while in transition; and identify components you may be missing out on.
-  Well defined milestones and deliverables, along with training, documentation and knowledge transfer; greatly accelerating **Time to Value (TTV)**.

Positioned for Success

A highly scalable services delivery methodology, following an Agile framework, with iterative processes; where an on-going customer feedback loop is incorporated into each project deliverable. As a result, adaptive adjustments are made, when and where required, for total quality management. The blended approach also provides structured oversight for an accelerated workflow, i.e. well defined roles and responsibilities, with clear and measurable milestones and deliverables.

Time Estimates

Deployment Size	Log Source Count	Duration
Small	300 Log-sources and 5k EPS + 10 use-cases	1 Week
Medium	5000 Log-sources and 5-50k EPS + 20 use-cases	2 - 3 Weeks
Large	>5000 Log-sources and >50k EPS + 30 use-cases	4+ Weeks

Note: Calculations are based on a complexity rating and an averaging scale. Via diligence, actual duration estimates may vary per a verified complexity score.

ASSESS

- Solution Design Workshops
- Key Stakeholders Interviews
- Baseline current deployment
- Evaluate Dependencies
- Define Criteria for Success

PLAN

- Scope of use-cases deployment
- Obtain Key Stakeholder Buy-In
- Establish incidents workflow
- Define Go-Live Testing Criteria

IMPLEMENT

- UBA installation
- Perform Baseline Tuning
- Implement custom use-cases
- Go-Live with validation Testing

OPTIMIZE

- Knowledge Transfer / Training
- Fine tuning of use-cases
- Steady-State Documentation

What to Expect:

Leveraging years of experience, across industry segments and geographic regions, our offering for IBM QRadar SIEM migration services is time-tested: eliminating guesswork, simplifying complexity, and ultimately, achieving the highest levels of success and satisfaction.

- Take your **SIEM deployment to the next level**
- Implement **meaningful and relevant use cases**
- Increased **security intelligence visibility**
- Enhanced **integrations and customized content**
- Roadmap for today, tomorrow, and beyond