**Demo Script**

|  |  |
| --- | --- |
| **Release Information** | |
| Use Case | UC 304 |
| Version | 1 |
| Related Documents | UBA\_SS\_Presentation.pptx |
| Pre-Requisites | UBA App UBA demo data |
| QRadar Version | 7.3.2 |
| **Demo Planning** | |
| Target Audience | SOC Analysts, SIEM Engineers |
| Main Demo Points | DSM Editor (Integrate new event source in CEF format) Integrate new component like Secret Server and develop use cases Dashboard configuration |
| Data sources | Secret Server Microsoft SQL LinuxOS |
| How much time | 30 minutes |
| Preparation Tasks | To use QRadar on Skytap:  - Deploy use case  To interactively run the presentation with your local QRadar:  - Copy SecretServerQ.tar.gz to your QRadar server in /root and extract content - Copy SecretServerW.zip to your Windows environment in folder C:\ and extract - Deploy the SSH Key on QRadar or use your own key |
| Clearance | Close offenses and wait for 5 minutes |
| **Demo Execution** | |
| Start the demo | Run use case |
| Total run time | Option 1 (run use case before presenting): 34 Seconds  Option 2 (run use case during presentation) |
| Time to wait |  |
| What to say | Some customers and especially many banks are required to monitor administrative access on their banking systems. The collected data overwhelms their teams. At best they can perform random tests. How can SIEM and especially UBA help to improve this situation? That is all explained by the presentation: Use Case 1:  It shows how SIEM can immediately re-act if there is a policy violation on a critical server. Highlight, that QRadar can limit this monitoring to critical systems to avoid too many FPs in the SOC.  Phase 1: Shows how it should be, i.e. the admin gets approval and then accesses the critical server 🡺 no offense Phase 2: Direct access to the critical server without approval, i.e. there is no secret server checkout before 🡺 offense Phase 3: Admin connects directly to secret server’s DB. This is not detected by secret server but QRadar receives a MS-SQL event. 🡺 offense (mention that this can be further tuned by adding additional criteria. We should not open an offense by any connect).   Use Case 2:  That use case elaborates UBA functionality. UBA provides the insight which session logs should be investigated. There is report (search @SecretServer: Risky Administrators) that lists admins which are reported by UBA. You can see this data also in the Pulse PAM dashboard. It is based on events generated by UBA in case a user is above risk threshold.   The other use cases are just to explain what can be done in UBA and SIEM to further support our customers. In the current version these use cases are not implemented. |