Threat Protection

Last updated by | Soma Jagadeesh | Jan 11, 2021 at 12:20 PM PST

Contents

Threat Detection and VA

Q: Is there a White List? (-No) Why?
A: One of the trickiest challenges is a malicious insider or former employees - they already have the credentials. For that reason, we rely on anomaly detection methods. If a user had a reason in the past to approach a database but the fact he is approaching it now is an anomaly, we want to alert about it. Having a allow list may leave backdoors for former employees, and indeed using that algorithm we helped to catch those incidents.

Q: The alert was activated on a principal user I already used before for the same server, why is that?
A: The anomaly algorithm is looking on a time frame window if you haven't used that user for a while now the algorithm may assume the user is out of use and alert on it when it appears again.

Q: The alert was activated on a principal user I'm using those days regularly, why is that?
A: The alert works on a server level, meaning that if you have a principal user that constantly approaches various of servers but didn't approach the particular server that was alerted on a regular basis, an anomaly will be detected. You may consider a compartmentalization approach in which even legitimate user's access to data is limited to what is required regularly. Another option is that we have a mistake in our algorithm and you are welcome to approach us with the details 😛

Q: I can't recognize the unfamiliar principal and I don't have auditing option turned ON at the server \ auditing didn't helped me to recognize the user, can you help me?
A: We are sorry but we share with you all the information we have. If we had more to tell you we would do so. We kindly recommend to turn on auditing for full investigation experience at least on servers that include important databases. If you do have auditing and still can't understand the incident you are welcome to consult us and we will try to help out of our experience, but probably you know your DBs and the normal activities for them the best.

How good have you found this content?

🙂 🙁