USE CASE: DETECTING APTS AND EXTERNAL HACKERS

A retail company unintentionally scheduled their Varonis risk assessment during the same week as an unrelated penetration test. The pentester compromised a service account on a Windows file server and was slowly and stealthily opening files of interest.

The pen tester's inconspicuous activity tripped a threat model in DatAlert designed to detect "low-and-slow" attacks. Even though the service account had legitimate access to the files, Varonis identified the subtle yet meaningful deviation in that service account's behavior.

How do you help with APTs and hackers that manage to get inside my network?

Varonis has threat models for each phase of the cyber kill chain—from detecting recon tools and binaries in strange locations, alerting on excessive account lockouts and access denied events, to abnormal file access.

DatAlert threat models detects when an insider isn't behaving normally, which is usually a sign that their account has been compromised by a hacker.

Varonis doesn't just profile end user accounts—we profile every executive, system and service account as well. Service accounts in particular are a favorite target of attackers – they usually have some level of file system or application access and can be used to probe or accumulate data for exfiltration.

Varonis looks for suspicious activity compared to an account's own historical baseline and across accounts. If multiple admin or service accounts generate an abnormal number of account lockouts compared to what's normal for that cohort, it might indicate that a hacker is trying to escalate privileges.

Relevant DatAlert threat models

- Abnormal behavior: accumulative increase in lockouts across end-user accounts
- Abnormal behavior: accumulative increase in lockouts for individual end-user accounts
- Abnormal behavior: accumulative increase in access to idle data
- Abnormal behavior: accumulative increase in access to idle and sensitive data
- Potential masked intrusion: system binaries found in unusual locations
- Recon tools detected