Managing *nix system user account behavior

Privileged user account behavior can cause problems on any business system and must be carefully managed. Your *nix systems are often critical to manage in this way as they tend to host important services. Part of your role is to ensure best practices on your systems when it comes to user accounts. This involves actively managing accounts and passwords, implementing least privilege, and controlling account access.

You want to use your Splunk deployment to track actions and events that are important for user account behavior management. This will allow you to understand if user error is the cause of malfunctions or if security has been compromised. You can use Splunk software to monitor everything on your *nix systems, from basic logon behavior to privileged behavior, such as the use of sudo commands.

Data required

*nix: Security logs

How to use Splunk software for this use case

You can run many searches with Splunk software to manage *nix system user behavior. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Successful logins to a *nix server
- Use of sudo commands on a server

Next steps

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at your organization or become new standard processes. These processes commonly impact success with this use case:

- Authentications that need to be tracked for compliance and security reasons
- Visibility to success and failed logons for your help desk center

Measuring impact and benefit is critical to assessing the value of IT operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Failed authentications over time
- Authentications by privileged users
- Authentications by privileged users on critical assets
This use case is also included in the IT Essentials Learn app, which provides more information about how to implement the use case successfully in your IT maturity journey. In addition, these Splunk resources might help you understand and implement this use case:

- Tech Talk: Get monitoring tricks for all your *nix part 1
- Tech Talk: Get monitoring tricks for all your *nix part 2