Monitoring Windows account access

Your organization uses Microsoft products and services as part of its information technology in support of your business. Account access is important to track to ensure users are able to access the systems needed to do their work. User accounts and service accounts are often also monitored for security reasons, so work done for one domain can help the other. You need a few basic searches related to Windows account access that can help both your team and the security team work more efficiently.

You can use Splunk software to monitor authentication to endpoints and troubleshoot account lockouts. You can also generate reports that support compliance reporting efforts around accounts and other Windows related components.

Data required

- Windows event logs
- System log data

How to use Splunk software for this use case

You can run many searches with Splunk software to monitor Windows account access. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Windows account activity overview
- Windows account lockouts
- Windows Zombie account lockouts
- Windows service account login attempts
- Baseline of user logon times
- Authentication logs for an endpoint

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:

- Active Directory group policies administration
- Identity and Access Management systems administration (e.g., OneLogon, Okta, etc.)

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:
• Count of Zombie account lockouts: Number mitigated per unit of time
• A reduction in the time taken for any of the following:
  ◦ Mean time to user account lockout discovery and resolution
  ◦ Mean time to detect (MTTD) problems
  ◦ Mean time to investigate
  ◦ Mean time to resolution
  ◦ Time to provide attestation to regulatory requirements related to user accounts, such as CIS Control 16

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:

• Blog: Peeping through Windows (logs)
• Conf Talk: Security visibility through Windows endpoint analytics
• Whitepaper: The Essential guide to AIOps
• Tech Brief: Artificial intelligence for IT Operations (AIOps)
• Analysis Report: Market guide to AIOps platforms
• Tech Talk: My start will go on: Splunk's TA for Windows Part 1
• Tech Talk: My start will go on: Splunk's TA for Windows Part 2