Brute force access behavior detected

Brute force access is a common attack vector. You want to monitor your security controls and prove your GDPR compliance by detecting brute force (or password guessing) attacks on GDPR-tagged systems.

Required data

Authentication data. This sample search uses Windows Security Logs. You can replace this source with any other authentication data used in your organization.

Procedure

1. Identify all relevant IT assets from a data mapping exercise conducted by the Data Privacy Officer’s team. These are all IT assets that are relevant to the full audit trail of data processing activities. This includes not only data stores and repositories that house sensitive personal data (PD) and personally identifiable information (PII), but also any technologies that are involved in the processing, storage, transmission, receipt, rendering, encrypt/decrypt, relaying, and handling of such data in any capacity.

2. Ensure that those assets are configured properly to report logging activity to an appropriate central repository.

3. Use your data mapping results to build a lookup that associates systems to their system category. At a minimum, the lookup must contain the host field mapped to a GDPR (or other compliance) category.

4. Run the following search. You can adjust this query based on the specifics of your environment.

   ```splunk
   source=*\WinEventLog:Security* user=* user!="" | stats count(eval(action="success")) AS successes count(eval(action="failure")) AS failures BY src dest | where successes>0 AND failures>100 | lookup <name of lookup created in step 3 above> host AS dest | search category=*  
   ```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>source=&quot;<em>\WinEventLog:Security</em>&quot;</td>
<td>Search only Windows security data.</td>
</tr>
<tr>
<td>split count(eval(action=&quot;success&quot;)) AS successes split count(eval(action=&quot;failure&quot;)) AS failures BY src dest</td>
<td>In this example, we specify the WinEventLog but your environment may need a different source type or you may only need tag=authentication.</td>
</tr>
</tbody>
</table>
Splunk Search

user=* user!=""

| stats count(eval(action="success")) as successes
count(eval(action="failure")) as failures by src dest

| where successes>0 AND failures>100

| lookup <name of lookup created in step 3 above> host as dest

| search category=*  

Explanation

Omit results where the user field value is not set.

Count how many events there are when the action was a success or when the action was a failure.

Set the threshold for the brute force attack with a filter for at least one success and more than 100 failures.

This value may need to be adjusted depending on risk tolerance or other unique conditions in your environment.

Use this lookup to determine if the system under attack is in scope for GDPR.

Filter for events that have a value in the category field.

Next steps

The output of the search displays the source, the time, the number of successes, and the number of failures when failures have been more than 100.

When this search fires, the immediate concern is that the brute force search was successful. See if it is coming from a host that typically logs in with that account to make sure it is not just coincidental, and then reset the password for any compromised accounts and look for any other places where that username was used.

Additionally, you should monitor the mapped IT assets changes in logging status, adjust for known outages, and prioritize incident response for any failures to report by hosts that are not scheduled for downtime.

**GDPR Relevance:** Under the GDPR, monitoring and demonstrating that security controls are effective is required by Article 32, therefore immediate awareness of any brute force attempts is critical to maintaining compliance posture. Demonstrating that any such attempts have not been successful will help to prove compliance for data privacy audits initiated by data privacy authorities (Article 58) and also help counteract compensation claims (Article 82).

You can also watch this search run and learn about more next steps in the following video.
For more great content from the Splunk Education and Training team, check out Splunk How-To on YouTube or sign up for a course.

Finally, you might be interested in other processes associated with the Complying with General Data Protection Regulation use case.