**Security Event Configuration in Pega**

The security event configuration feature is a part of security information and event management (SIEM), which combines security information management (SIM) and security event management (SEM). Use the Security Event Configuration landing page to configure the logging of security events so that you can diagnose system issues and demonstrate compliance to auditors.

Security events includes actions performed by any requestor who access the application, data accesses or changes, changes to security policies or security- related rules or landing pages, and so on. With the logged security events you can then monitor inappropriate access to your data or system.

All Security Events include the following information

1. Date and time
2. Application Name
3. Node
4. IP Address
5. Operator ID
6. Event class(authentication and authorization)
7. Event type

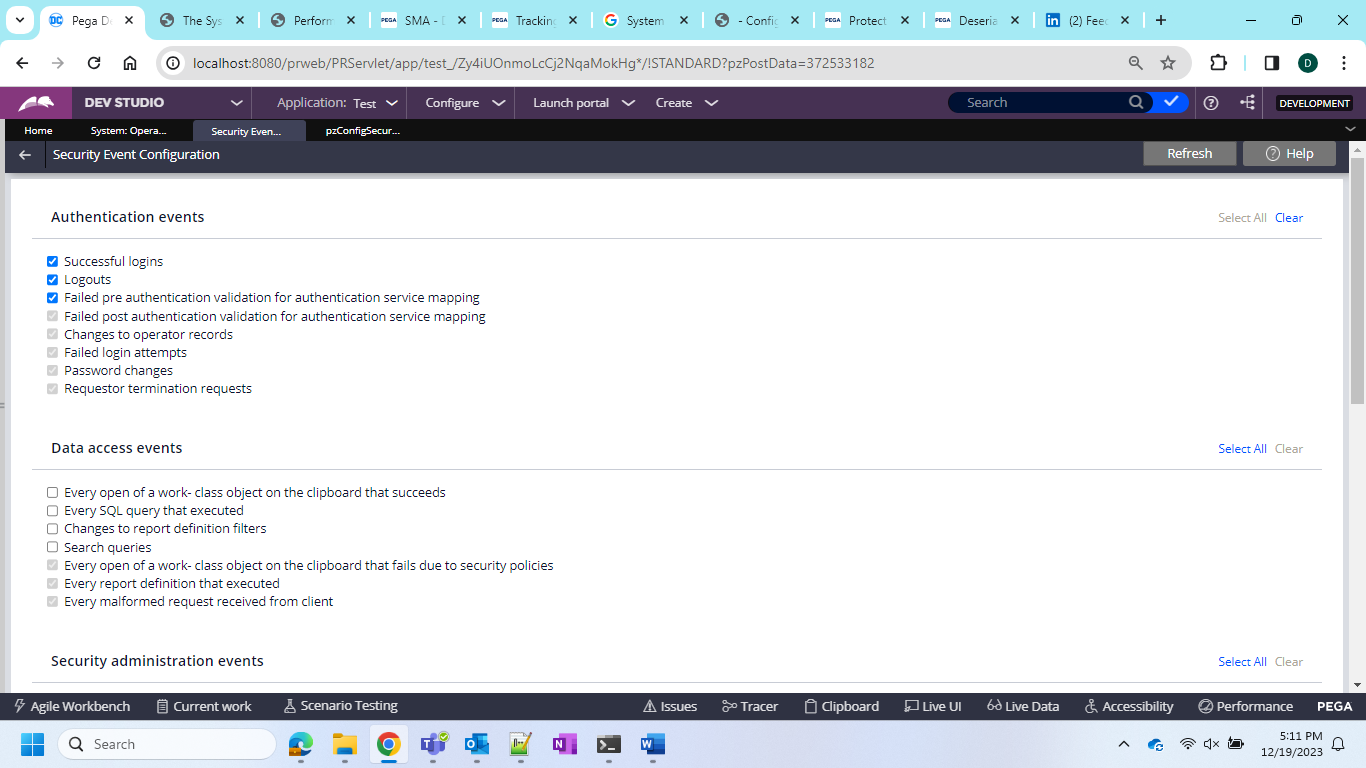
Authorization events can also include the following information

1. The entered search string
2. Report name, class, and filter condition.
3. The class, ID, and class- of the case state:

* Open
* Unopened
* Blocked by an access policy

So in order to check which logs need to be configured and we use the wizard in order to see which you can select and where you can see

So as per configuration dialog box we can see the things which can be seen in logs



A computer screen with a white screen

Description automatically generated

Now after the configuration we can see In the logs

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

And in the logs now we can see the login success in the logs and security event in logs we can see the entry

