**SAP Used Cases in SIEM (Security Incident and Event Monitoring)**

**CASE-1 -**

|  |  |
| --- | --- |
| Name | Failed Logon Attempts for Dialog and RFC on Production |
| Description | SAP User has 9 or more failed login attempts on production within a SPAN of 2 hours in a 24-hour window. Urgency Medium |
| Remediation | Failed logins of >9 on production within a SPAN of 2 hrs |

|  |  |
| --- | --- |
| Query Used | index=ABC reason=52 SID=P\*  | stats count(USERID) as Failed\_Logon\_Count by USERID TERMINALID APPSERVER MESSAGETEXT SID PROGRAMNAME  | where Failed\_Logon\_Count>8 |

**CASE-2 –**

|  |  |
| --- | --- |
| Name | SAP Access to Functional models in Production |
| Description | Users should not be granted SE37/SE38 access. Though they cannot change the code, they can directly execute it. Authorization with activity they can also execute programs or function modules and they can "skip" the authority checks. This can create users or assign SAP\_ALL to themselves without trace.  Rule checks for all non-Firefight/non-SAP Security accounts with TCODE SE37/SE38 transaction starts and Production. |
| Remediation | SE37/SE38 table execution can skip authority checks leading to elevated privileges. Please determine if use was legitimate by investigating with the TCS SAP Security Team: |

|  |  |
| --- | --- |
| Query Used | index=ABC | eval TCODE=trim(TCODE) | search NOT TCODE IN (SE38 SE37) SID=P\* WPTYPE!=B (MESSAGETEXT="\*Transaction SE38 Start\*" OR MESSAGETEXT="\*Transaction SE37 Start\*")  | stats count(USERID) as User\_Count by USERID TERMINALID APPSERVER MESSAGETEXT SID PROGRAMNAME |

**CASE-3 –**

|  |  |
| --- | --- |
| Name | SAP Execution of ZCMD |
| Description | ZCMD, is a custom OS external command, that allows an SAP user to execute arbitrary OS commands as SAP administrator or SAP Service administrator. Using this custom command, a remote authenticated attacker will be able to execute arbitrary operating system commands, leading it to a Privilege Escalation. |
| Remediation | ZCMD execution is not authorized with exception of processes already using it. |

|  |  |
| --- | --- |
| Query Used | index=ABC ZCMD |eval Time=strftime(\_time,"%c") |dedup MessageVar2  |table Time,MessageText,MessageVar2 Client SID JobName  |rename MessageText as "Message" , MessageVar2 as "Machine Name" |

**CASE-4 –**

|  |  |
| --- | --- |
| Name | SAP OS Command Execution on Production |
| Description | Sm69 is an SAP t-code where you can define OS commands and arbitrary execution of command execution with OS level COPY / delete/ move etc. In Prod no user should have direct access. But some SAP background process may need t-code access. |
| Remediation | SE69 table execution can define OS command execution and arbitrary execution of commands with OS level COPY/ Delete etc. |

|  |  |
| --- | --- |
| Query Used | index=ABC TCODE IN (SM69) MESSAGETEXT="Transaction SM69 Start\*"  | stats values(MESSAGETEXT) by USERID TERMINALID PROGRAMNAME \_time |

**CASE-5 –**

|  |  |
| --- | --- |
| Name | Unauthorized Access Attempts |
| Description | End users should not have access to SE16 in SAP because the necessary authorizations are not present to limit access to sensitive data. Depending on the authorizations given, end users could possibly change tables and configuration directly. |

|  |  |
| --- | --- |
| Query Used | index=ABC "auth. check: failed" TCODE=SE16 PARAMETER2=03 SID=P\* | stats values(MESSAGETEXT) by USERID PARAMETER1 TERMINALID WPTYPE TCODE APPSERVER PROGRAMNAME SID |

**Sample Output:**

**CASE-6 –**

|  |  |
| --- | --- |
| Name | SAP Usage of Critical SAP In-built User ID's |
| Description | SAP comes with some inbuilt user ids SAP\* DDIC SAPTMS SAPCPIC. As best practice it is recommended to lock these ids and not use except in case of emergency. These ids also have very powerful access and if any unauthorized user use these ids, they can get access to SAP application which otherwise they are not authorized to perform. |
| Query Used | index=ABC | eval MESSAGEGROUP=trim(MESSAGEGROUP),MESSAGESUBGROUP=trim(MESSAGESUBGROUP),USERID=trim(USERID) | search USERID IN (SAP"(\*)" DDIC SAPTMS SAPCPIC) AND ((MESSAGEGROUP=BU AND MESSAGESUBGROUP=2) OR (MESSAGEGROUP=AU AND MESSAGESUBGROUP IN (8 7 9 A B D R S T U))) AND (SID=P\*) | table USERID TERMINALID APPSERVER MESSAGETEXT SID PROGRAMNAME |

**CASE-7 –**

|  |  |
| --- | --- |
| Name | SAP Change on user done by non-Security user. |
| Description | As per policy any dialog user creation or role assignment is automated via IdM. Security team manually maintain system or communication ids. Any attempt by unauthorized user to change user ids to gain additional access should be tracked. This can happen in scenarios where someone inadvertently has user management access, or someone was able to successfully hack systems to gain unauthorized access. |
| Query Used | index=ABC | eval MESSAGEGROUP=trim(MESSAGEGROUP),MESSAGESUBGROUP=trim(MESSAGESUBGROUP),USERID=trim(USERID) | ((MESSAGEGROUP=BU AND MESSAGESUBGROUP=2) OR (MESSAGEGROUP=AU AND MESSAGESUBGROUP IN (8 7 9 A B R S T U))) AND (SID=P\*) | table PROGRAMNAME USERID MESSAGEGROUP MESSAGESUBGROUP \_time PARAMETER1 MESSAGETEXT |

**CASE-8 –**

|  |  |  |
| --- | --- | --- |
| Name | | SAP Debugging session initiated in production by dialog User. |
| Description | | Debugging of code in production should be exercised only in case of some critical bug analysis which can't be reproduced in lower environments. Debugging currently is only permitted in firefighter ids. If any user or developer is debugging in production, it needs to be tracked and analyzed. There is security implication of debugging in production like user can see unauthorized data, can modify production data. |
| Query Used | index=ABC | eval MESSAGEGROUP=trim(MESSAGEGROUP),MESSAGESUBGROUP=trim(MESSAGESUBGROUP),USERID=trim(USERID)| search ((MESSAGEGROUP=BU AND MESSAGESUBGROUP=Z) OR (MESSAGEGROUP=CU AND MESSAGESUBGROUP IN (K L M N O P Y))) ( SID=P\*) | table PROGRAMNAME USERID MESSAGEGROUP MESSAGESUBGROUP \_time LogonMethod method PARAMETER1 PARAMETER2 PARAMETER3 | |

**CASE-9 –**

|  |  |  |
| --- | --- | --- |
| Name | | Download of critical HR data from SAP Application Description |
| Description | | Download of HR data from production boxes should be limited and granted to only few authorized users. If someone is downloading HR data multiple times without any valid business reason that will need investigation to determine purpose for which user downloaded HR data. |
| Query Used | index=ABC PROGRAMNAME IN (/1BCDWB/DBPA0\*) (SID=P\*) | table PROGRAMNAME USERID MESSAGEGROUP MESSAGESUBGROUP \_time PARAMETER1 PARAMETER2 PARAMETER3 SID | |

**CASE-10 –**

|  |  |  |
| --- | --- | --- |
| Name | | Download of Critical Security Data from SAP Application |
| Description | | Download of security data from production should be limited and granted to only security team. If someone is downloading security data multiple times without any valid business reason that will need investigation to determine purpose of user downloaded security data. |
| Query Used | index=ABC PROGRAMNAME IN ( /1BCDWB/DBPAUSR\* /1BCDWB/DBPAAGR\* ) (SID=P\*) | table PROGRAMNAME USERID MESSAGEGROUP MESSAGESUBGROUP \_time PARAMETER1 PARAMETER2 PARAMETER3 SID | |

**CASE-11 –**

|  |  |  |
| --- | --- | --- |
| Name | | Changes in Audit Configuration Settings in Production |
| Description | | Download of security data from production should be limited and granted to only security team. If someone is downloading security data multiple times without any valid business reason that will need investigation to determine purpose of user downloaded security data. |
| Query Used | index=ABC | eval MESSAGEGROUP=trim(MESSAGEGROUP),MESSAGESUBGROUP=trim(MESSAGESUBGROUP),TCODE=trim(TCODE) | search TCODE=SM19 MESSAGEGROUP=AU MESSAGESUBGROUP IN ( E F I J ) (SID=P\*) | table PROGRAMNAME MESSAGETEXT USERID MESSAGEGROUP MESSAGESUBGROUP \_time method PARAMETER1 PARAMETER2 PARAMETER3 TCODE | |

**SAP Alerts in SIEM (Security Incident and Event Monitoring)**

**ALERT-1 –**

|  |  |
| --- | --- |
| Name | Failed Logon Attempts on Dialog and RFC for Service Accounts |
| Description | End users should not have access to SE16 in SAP because the necessary authorizations are not present to limit access to sensitive data. Depending on the authorizations given, end users could possibly change tables and configuration directly. |
| Run & Trigger. | Runs Every 24 hours and results would be emailed to respective individuals and groups. |

|  |  |
| --- | --- |
| Query Used | index=ABC reason=53 SID=P\* USERID!=SMDAGENT\_PGS AND USERID!=ALE\* AND USERID!=\*ADM | stats count(USERID) as Failed\_Logon\_Count by USERID TERMINALID APPSERVER MESSAGETEXT SID PROGRAMNAME | where Failed\_Logon\_Count>2. |

**ALERT-2**

|  |  |
| --- | --- |
| Name | Alert for table SM01 execution on Production Systems |
| Description | Having access to SM01 would result in users to lock and unlock tables which is a security violation. Other than actual business used case this functionality should not exist in daily operations. Malicious intent can cause users to view tables (e.g.: bank accounts, name, number etc.) |
| Run & Trigger. | Runs Every 24 hours and results would be emailed to respective individuals and groups. |

|  |  |
| --- | --- |
| Query Used | index=ABC TCODE=sm01 SID=P\* MESSAGETEXT="Transaction SM01 started\*" NOT USERID IN | stats values(MESSAGETEXT) by USERID TERMINALID PROGRAMNAME. |

**ALERT-3**

|  |  |
| --- | --- |
| Name | SAP Security Audit Administrator User Account Status |
| Description | Alert describes any user account activity with lock=false and lockreason=0  Alert Details:  User account modified | USERACCOUNT.MODIFY | UACC.PRIVATE\_DATASOURCE.un:Administrator | | SET\_ATTRIBUTE: lockreason=[0], SET\_ATTRIBUTE: islocked=[false]#  Action Plan: Kindly verify if there are any activities using Administrator account. If not, proceed to lock it via User Admin page. |
| Run & Trigger. | Runs Every 5 minutes and is automated to generate a Service Now ticket to respective group. Copy of results are also emailed to respective individuals and groups. |
| Query Used | index=ABC sourcetype=sap\_java\_system host=xxx "UACC.PRIVATE\_DATASOURCE.un:Administrator" islocked="[false]" | table \_raw \_time |

**ALERT-4**

|  |  |
| --- | --- |
| Name | SAP Security local password policy settings in User Admin |
| Description | Local password policy settings in User Admin page. Ensure the value are comply with KC IT Standard 270-01 (<https://archer.kcc.com/apps/ArcherApp/Home.aspx>)  Alert Details: KCC20210407002 SAP Security local password policy settings in User Admin  What Happened: Local Password Policy Settings changed/modified  Current UME configuration | CUSTOMIZE| Modified non-secure Properties | ume.logon.security\_policy.password\_expire\_days=["91" -> "90"],  Action Plan: Kindly proceed to verify local password policy settings in useradmin page. Ensure the value are comply with KC IT Standard 270-01  (https://archer.kcc.com/apps/ArcherApp/Home.aspx) |
| Run & Trigger. | Runs Every 5 minutes and is automated to generate a Service Now ticket to respective group. Copy of results are also emailed to respective individuals and groups. |
| Query Used | index=ABC sourcetype=sap\_java\_system host=xxx "ume.logon.security\_policy" | table host  ume\_logon\_security\_policy\_auto\_unlock\_time  ume\_logon\_security\_policy\_enforce\_policy\_at\_logon  ume\_logon\_security\_policy\_lock\_after\_invalid\_attempts  ume\_logon\_security\_policy\_password\_alpha\_numeric\_required  ume\_logon\_security\_policy\_password\_expire\_days  ume\_logon\_security\_policy\_password\_history  ume\_logon\_security\_policy\_password\_impermissible  ume\_logon\_security\_policy\_password\_max\_idle\_time  ume\_logon\_security\_policy\_password\_max\_length  ume\_logon\_security\_policy\_password\_min\_length  ume\_logon\_security\_policy\_password\_mix\_case\_required  ume\_logon\_security\_policy\_password\_special\_char\_required  \_time |