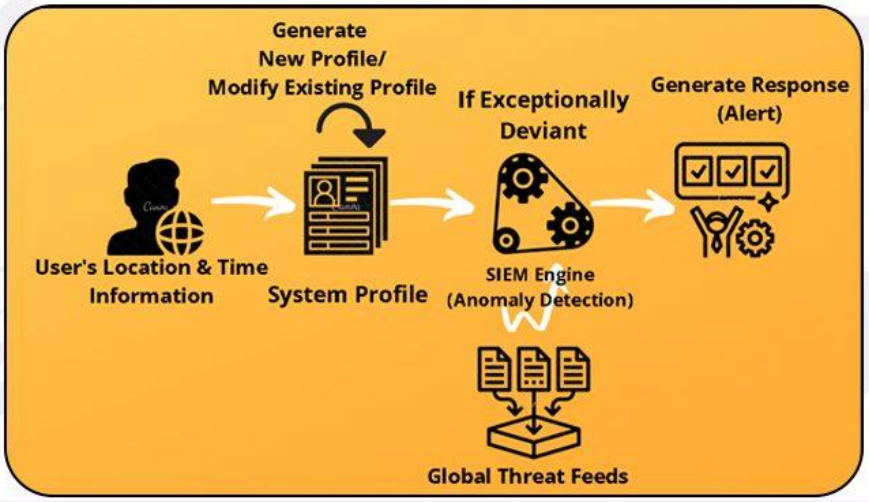
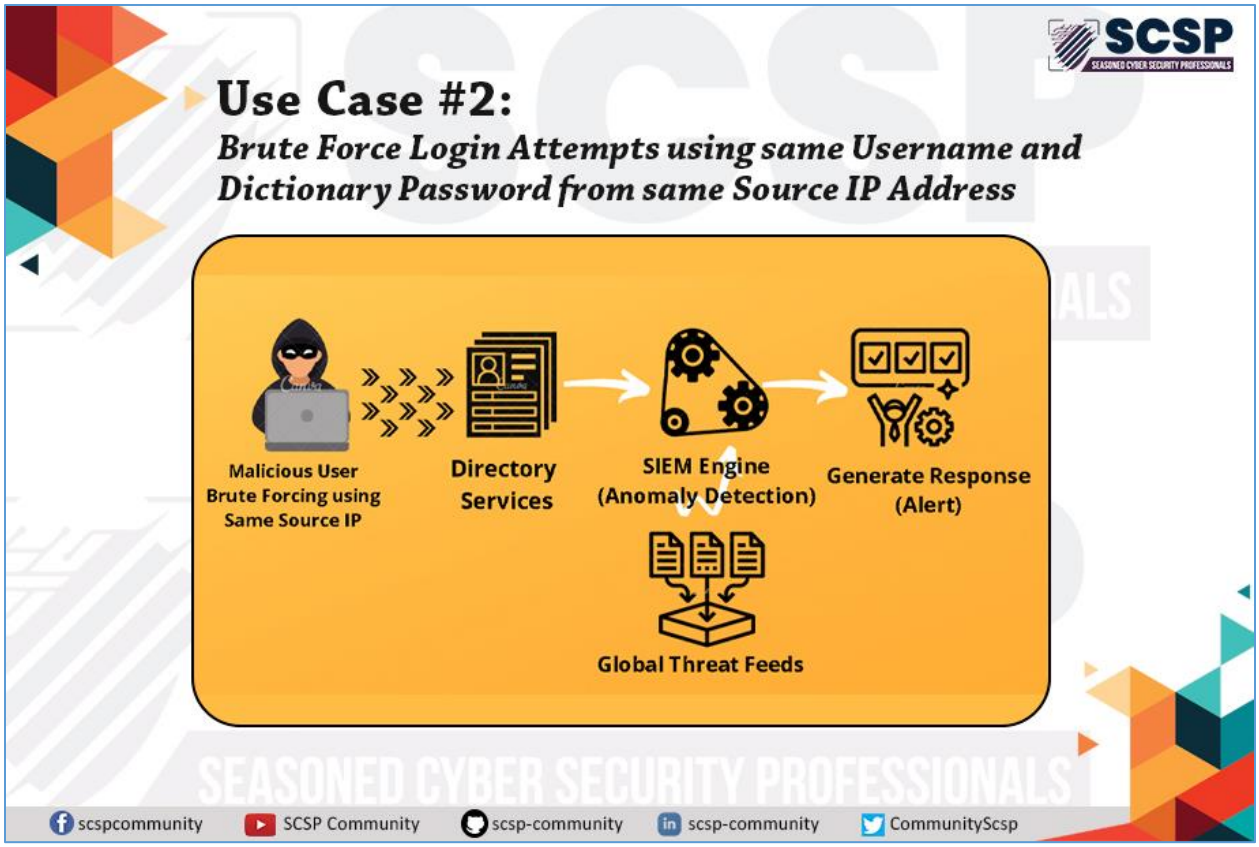

SCSP
SEASONED CYBER SECURITY PROFESSIONALS
SIEM Use Cases!
scspcommunity
SCSP Community
scsp-community
scsp-community
CommunityScsp

Use Case #1:

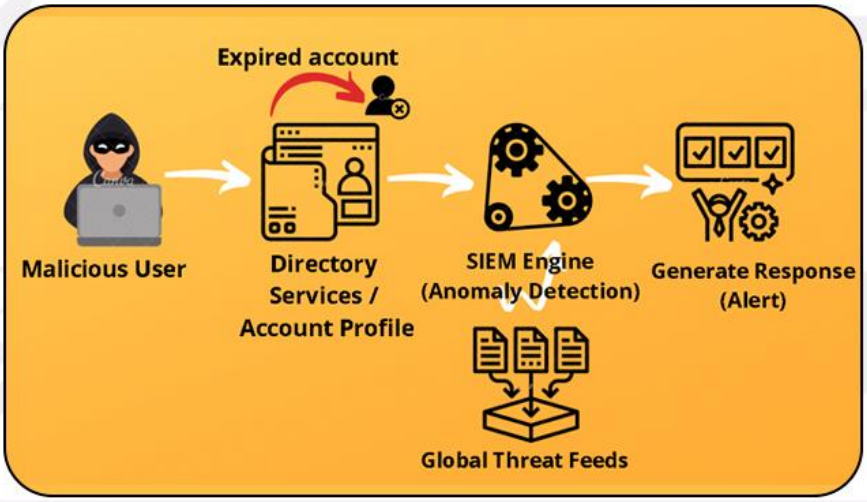
Unusual Login Activity from different Locations in short Time

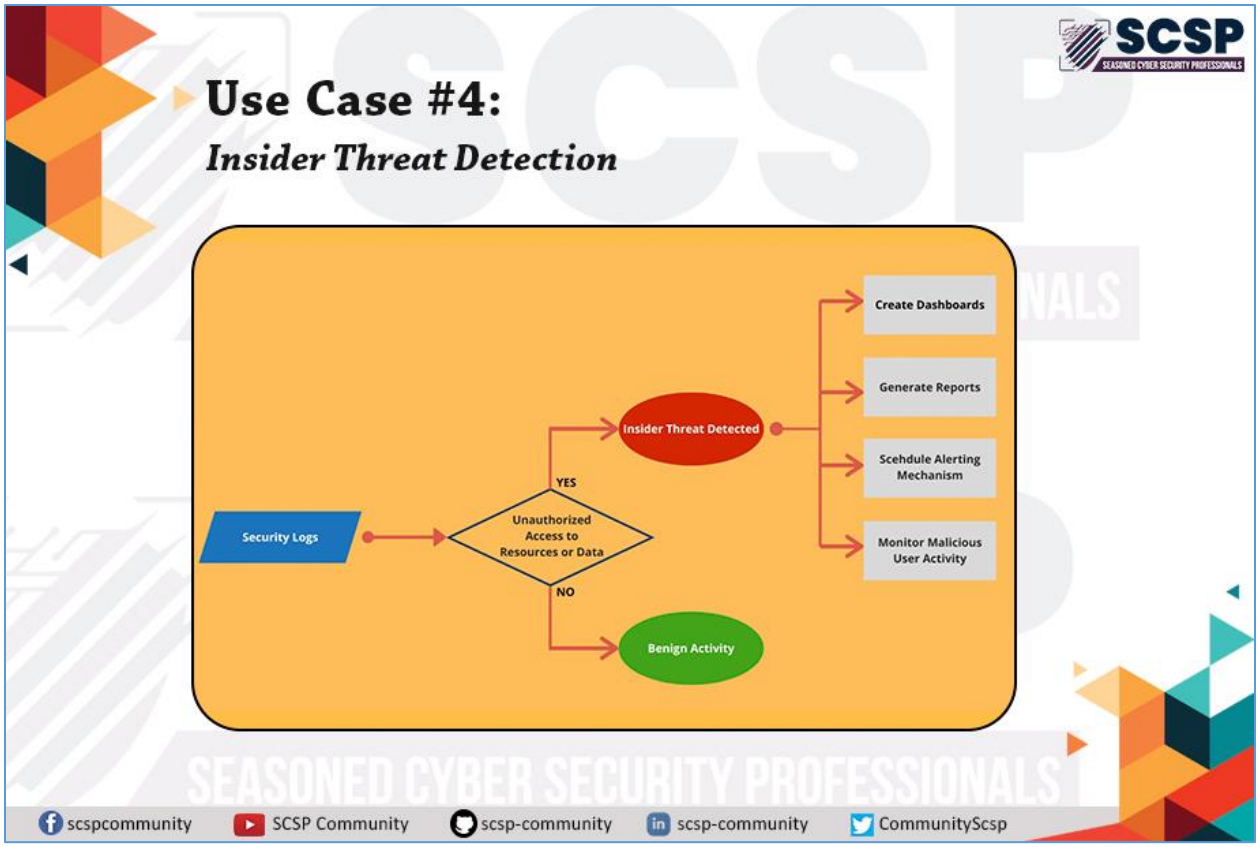


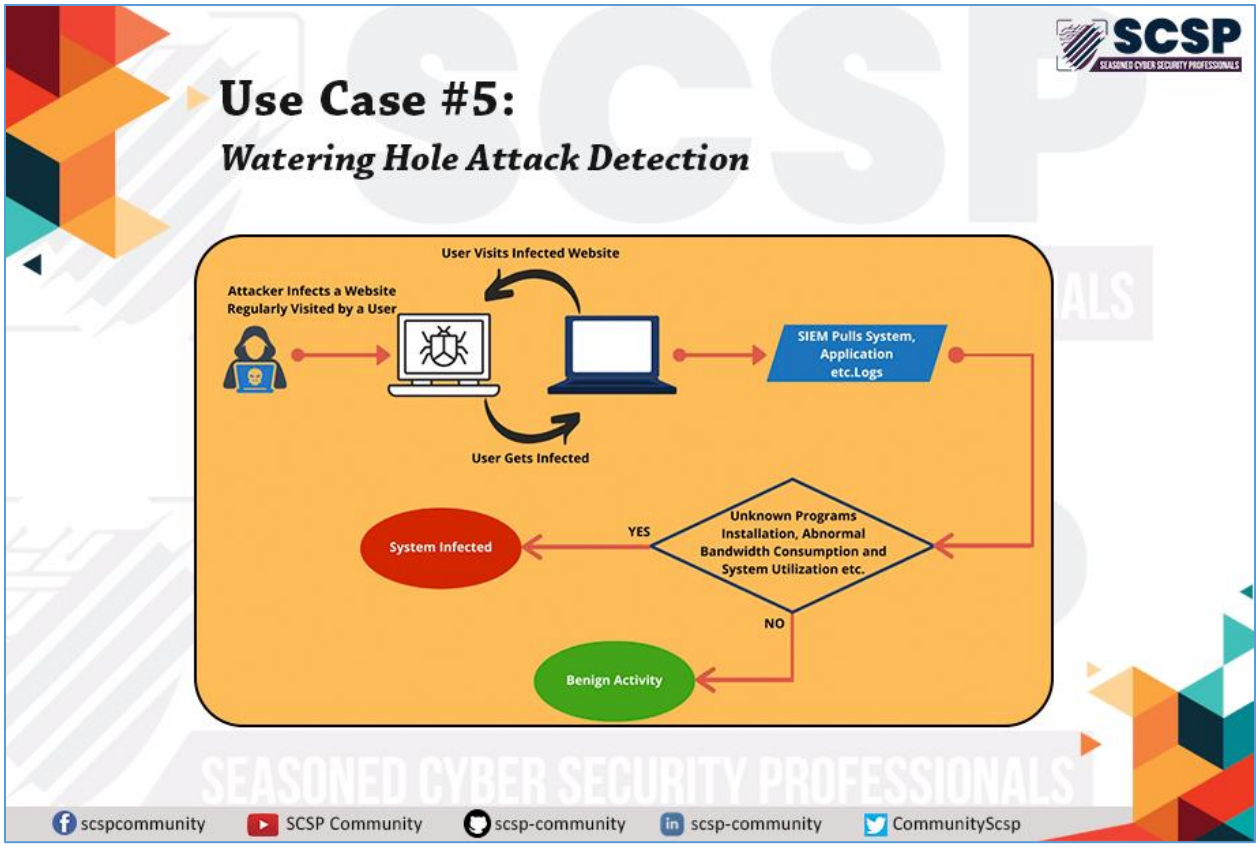

SCSP
SEASONED CYBER SECURITY PROFESSIONALS
Use Case #2:
Brute Force Login Attempts using same Username and Dictionary Password from same Source IP Address
Malicious User Brute Forcing using Same Source IP
Directory Services
SIEM Engine (Anomaly Detection)
Generate Response (Alert)
Global Threat Feeds
SEASONED CYBER SECURITY PROFESSIONALS
scspcommunity
SCSP Community
scsp-community
scsp-community
CommunityScsp

Use Case #3:

Logon Failure – Attempts made to logon using Expired Accounts.




SCSP
SEASONED CYBER SECURITY PROFESSIONALS
Use Case #4:
Insider Threat Detection
Security Logs
Unauthorized Access to Resources or Data
YES
NO
Insider Threat Detected
Benign Activity
Create Dashboards
Generate Reports
Scehdule Alerting Mechanism
Monitor Malicious User Activity
SEASONED CYBER SECURITY PROFESSIONALS
scspcommunity
SCSP Community
scsp-community
scsp-community
CommunityScsp


SCSP
SEASONED CYBER SECURITY PROFESSIONALS
Use Case #5:
Watering Hole Attack Detection
User Visits Infected Website
Attacker Infects a Website Regularly Visited by a User
SIEM Pulls System, Application etc.Logs
User Gets Infected
Unknown Programs Installation, Abnormal Bandwidth Consumption and System Utilization etc.
YES
System Infected
NO
Benign Activity
SEASONED CYBER SECURITY PROFESSIONALS
scspcommunity
SCSP Community
scsp-community
scsp-community
CommunityScsp