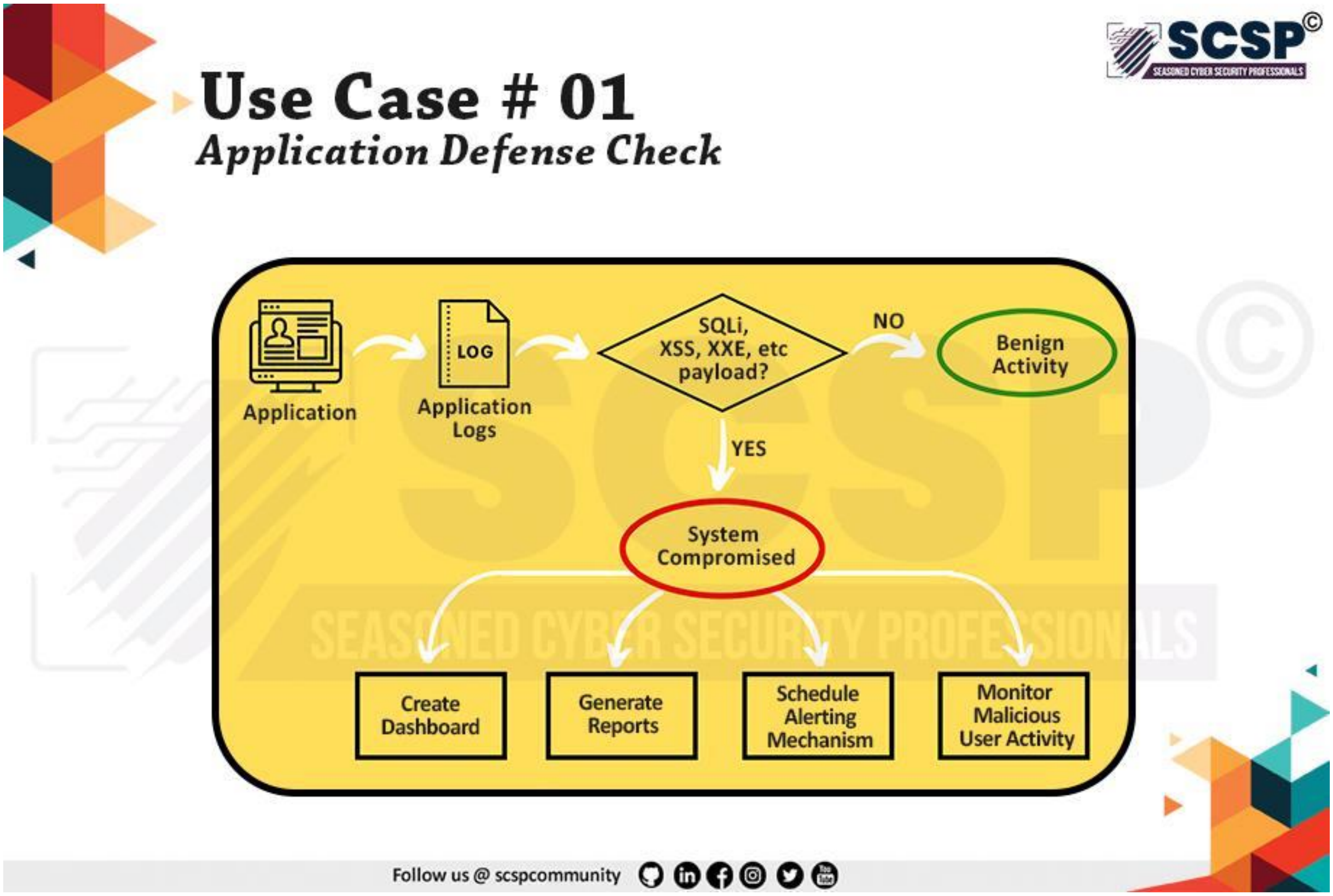
SCSP
SEASONED CYBER SECURITY PROFESSIONALS

SIEM Use Cases!

Part 3

scspcommunity   SCSP Community   scsp-community   scsp-community   CommunityScsp



Use Case # 01

Application Defense Check

Application

Application Logs

SQLi, XSS, XXE, etc payload?

NO

Benign Activity

YES

System Compromised

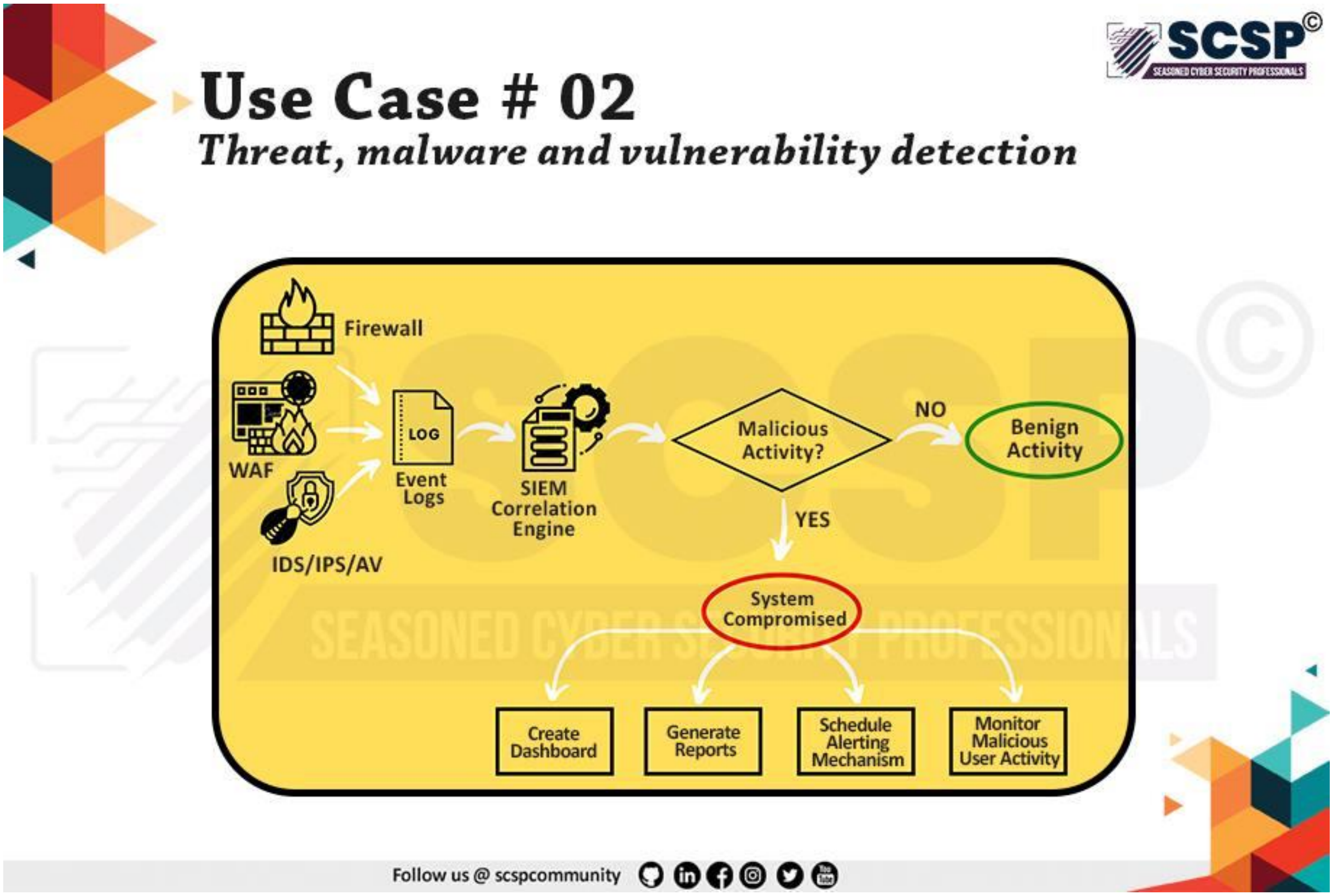
Create Dashboard

Generate Reports

Schedule Alerting Mechanism

Monitor Malicious User Activity

Follow us @ scspcommunity



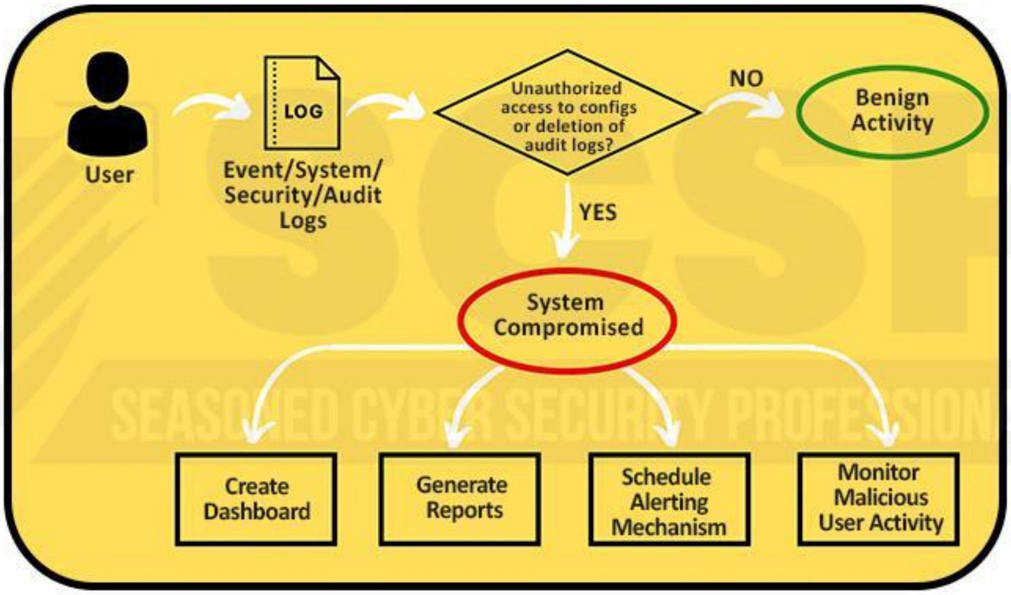
Use Case # 02

Threat, malware and vulnerability detection

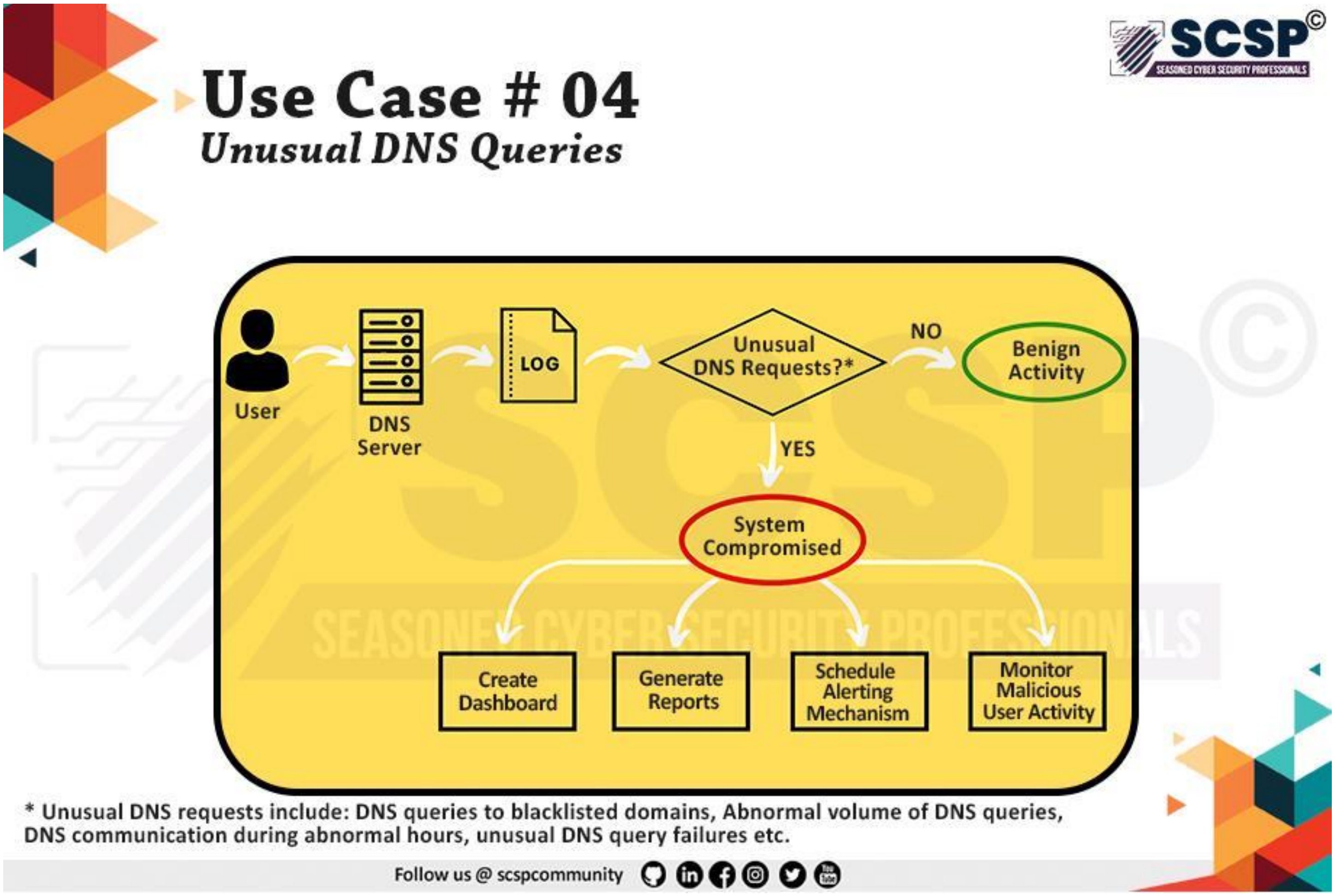
Follow us @ scspcommunity

Use Case # 03

Policy Related Activities/System Changes


User
LOG
Event/System/ Security/Audit Logs
Unauthorized access to configs or deletion of audit logs?
NO
Benign Activity
YES
System Compromised
Create Dashboard
Generate Reports
Schedule Alerting Mechanism
Monitor Malicious User Activity

Follow us @ scspcommunity

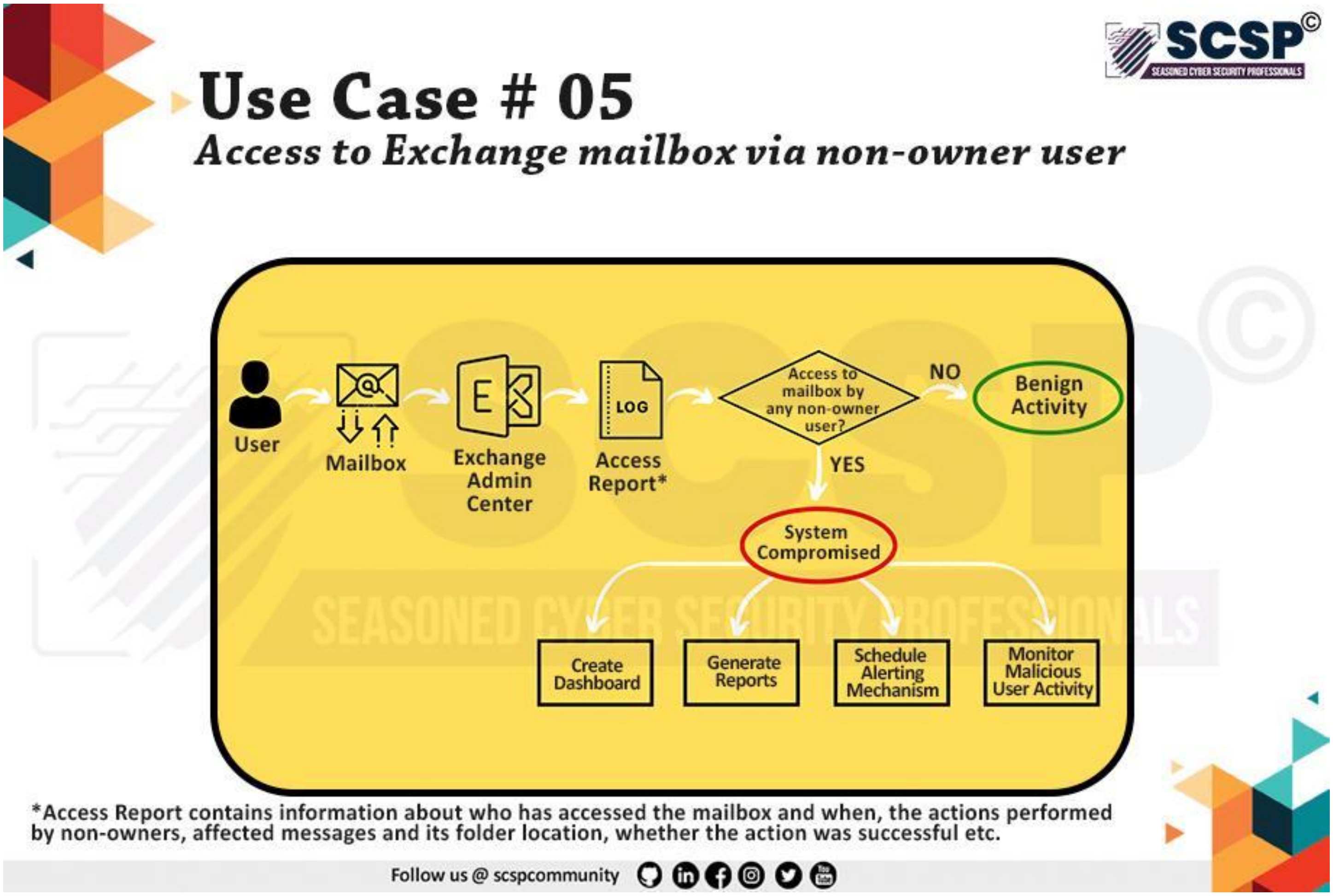


SCSP©
SEASONED CYBER SECURITY PROFESSIONALS

Use Case # 04

Unusual DNS Queries

* Unusual DNS requests include: DNS queries to blacklisted domains, Abnormal volume of DNS queries, DNS communication during abnormal hours, unusual DNS query failures etc.



SCSP©
SEASONED CYBER SECURITY PROFESSIONALS

Use Case # 05

Access to Exchange mailbox via non-owner user

*Access Report contains information about who has accessed the mailbox and when, the actions performed by non-owners, affected messages and its folder location, whether the action was successful etc.

Follow us @ scspcommunity