חרבות ברזל -

הרשאות rbac לחיילים

הקמת VM חקירה

מיפוי נכסי צהל באזור

מיפוי נכסי צהל באמזון

נוהל חקירת מכונה + סנפשוט מדיסק + memory dumps  
  
  
תיק חפיפה-

azure

חפיפת תקשורת  
identity  
 logicup/vm/storage accounts/sql - workloads  
resources

purview חקירות דאטה

חפיפת AWS

identity  
workloads  
resources

תיק מקורות חקירה-

לינק לwb של חוקי AWS שתועדו בconf

עמוד להצפת פערים

endpoints >indicators

חקירות דאטה - PURVIEW

exchange + emails investigations

common tables  
sentinel logs

wb upn + ip

identity

useful logicups

TI + TH

טמפלייט חקירה לפי IR CYCLE

דוגמה לטמפלייט חקירה לפי IR CYCLE

משימה להודיה-

טמפלייט חתמצים והצגה בדיונים  
תיק חפיפה לזוס כולל חפיפה מעשית (מחקר) וקורסים שעליו לבצע

טבלת משמרות עם ציד שחור

משימות רק לגנקין - להעביר מסמכים מעמדת חוץ או סוואנה להודיה/paw

קורסים - 508 מגנס וסיסו

זוס לוגיקאפים שרצים אחרי סגירת אירוע

שיחות אישיות לחיילים

לעבור על מסמך SC200 של עמית

מעבר למתחם של הצוות

ראיונות למגנסים חדשים

יצירת PAGE חדש לצוות בconf

זוס -

מבצוע SOC AWS - 40 high risk rules

אפיון וכתיבת חוקי כפג

יישום ותיעוד auto remediation

office365 defender policies ?

אכיפת bastion על vms - אחריות MCS

אכיפת pim על entra id roles - הרשאות directory אחריות MCS

defender for endpoint > indicators