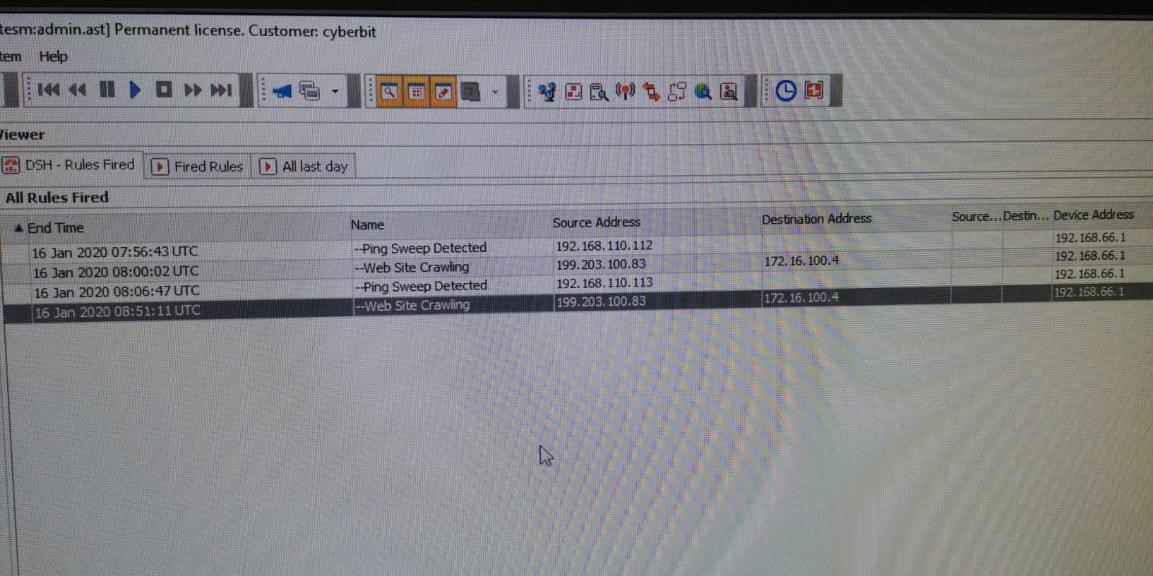
דוח אירוע

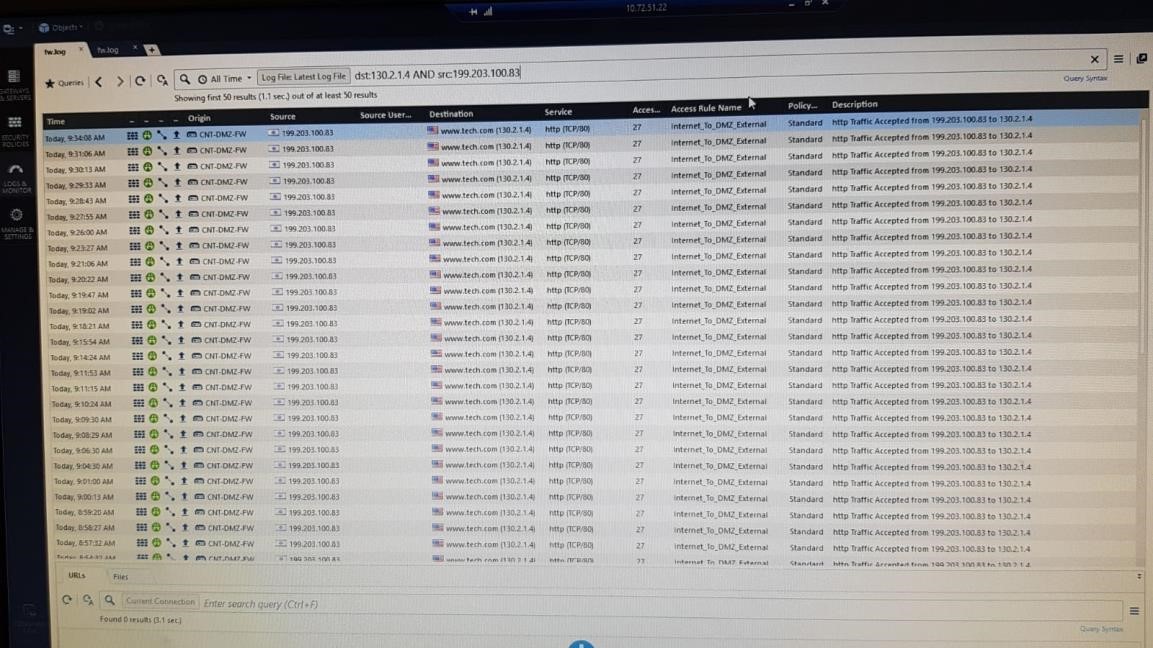
מגיש: דור לבקוביץ – 203565015

שם התרחיש - SQL Injection

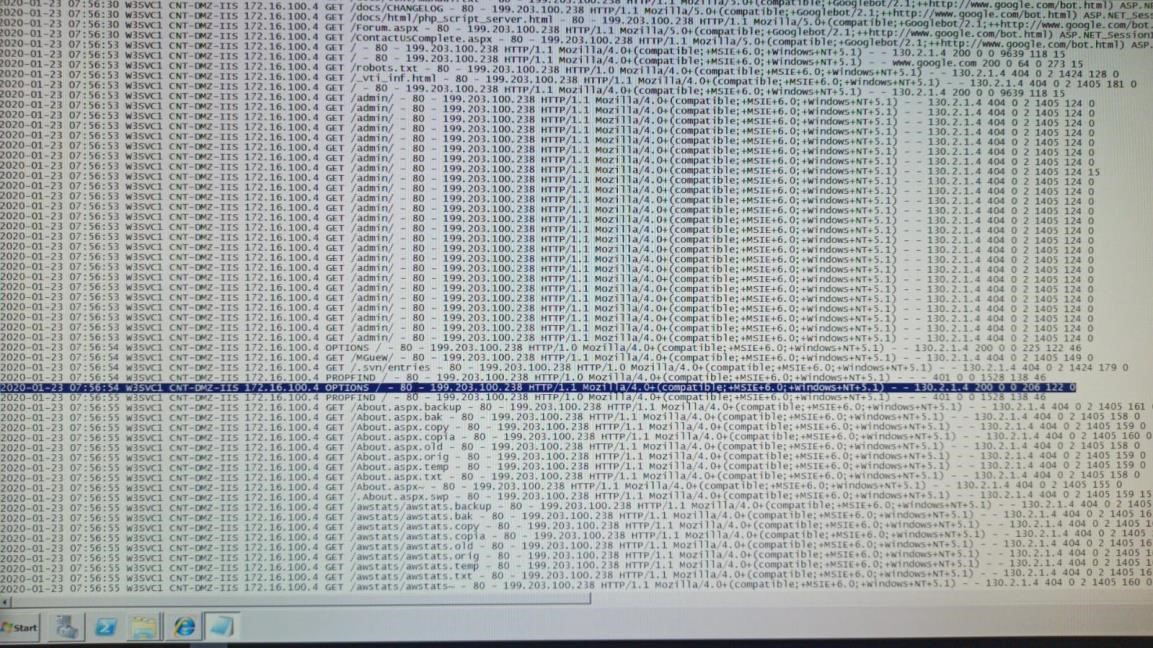
תהליך ההתקפה – תוקף נכנס לאתר האינטרנט של הארגון ודרך טופס יצירת הקשר הכניס פקודות SQL לשרת ממסד הנתונים על מנת לסרוק קבצים בשרת להפסיק תהליכים.

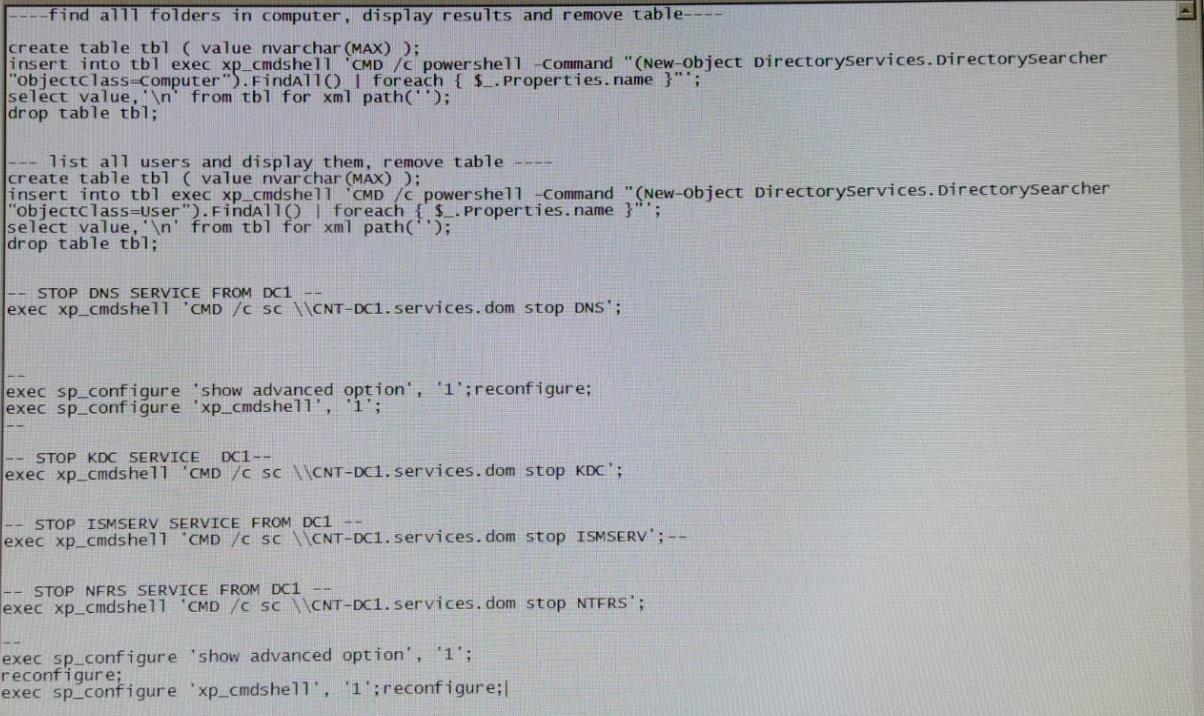
תהליך הזיהוי – לאחר בדיקה ראינו ב- ArcSight פעילות חשודה





נכנסו לשרת ולאחר בדיקה מעמיקה ראינו שם את כתיבת הפקודות בתוך הטופס יצירת קשר של האתר





תהליך ההגנה הראשוני – למנוע גישה לכתיבת פקודות SQL בטפסים פשוטים.

לחסום IP ששולח המון התראות בזמן קצר (מציף).

אופן ההתקפה – התוקף נכנס בעצם דרך טופס פשוט ושלח דרכו פקודות SQL ובכך לגרום נזק רב ל- DATABASE של הארגון.

כלים חדשים שפיתחתם/השתמשתם - אילו כלים השתמשתם/פיתחתם ומדוע – לא היה שימוש

אופן עבודת הצוות – עבדנו יחד והפעם היה שיתוף פעולה וסדר

חוסרים/קשיים/בעיות – חוסר הבנה בפקודות שלא הכרנו לפני