CYBER STRUGGLE
TASK- Securing the Motherland

Hazırlayan:
DCS001 Hakan ŞEN
Kasım 2023
Ankara

Hi Team,

Our headquarters received a crucial information note from an outsourced threat intelligence company about potential attacks. They are concerned about these threats, but our internal alert system has not detected any incidents. We have been using the TippingPoint IPS since our SOC implementation. An analysis report on these attacks is now expected.

In the report you need to include some dashboards presents below information:

Task 1 : You should monitor the severity of the suspicious activities and attack signatures alongside with the information such as its source, destination, geolocation and event name or any other information that you think it is needed. It would be beneficial to provide an explanation of attack signatures and how security devices utilize them.

Şüpheli faaliyetlere ilişkin olarak kullanılan ips üzerinden araştırma yapılmıştır. EventName loglar arasında parse edilmiş olarak gelmediğinden CEF format headerında alanın 5'inci bölümde olduğu bilinmesi nedeniyle ilgili alan için regular expression ile field çıkarılmıştır. Aynı durum EventSeverity içinde yapılmıştır.

Splunk Sorgusu:
index="endpoint" source="tippingPoint.cef" categorySignificance="/Suspicious" OR categorySignificance="/Hostile" OR categorySignificance="/Recon" |iplocation src |rex "^(?:[^|]*|){5}(?<EventName>[^|]+)|" |rex "^(?:[^|]*|){6}(?<EventSeverity>[^|]+)|" |stats count by src, dst,Country,City,EventName,EventSeverity

New Search

Save As | Create Table View | Close

```
index="endpoint" source="tippingPoint.cef" categorySignificance="/Suspicious" OR categorySignificance="/Hostile" OR categorySignificance="/Recon"
|iplocation src
|rex "^(?:[^|]*\|){5}(?<EventName>[^|]+)\|"
|rex "^(?:[^|]*\|){6}(?<EventSeverity>[^|]+)\|"
|stats count by src, dst,Country,City,EventName,EventSeverity
```

All time

✓ **67,987 events** (before 11/4/23 6:50:13.000 PM) No Event Sampling | Job | Verbose Mode

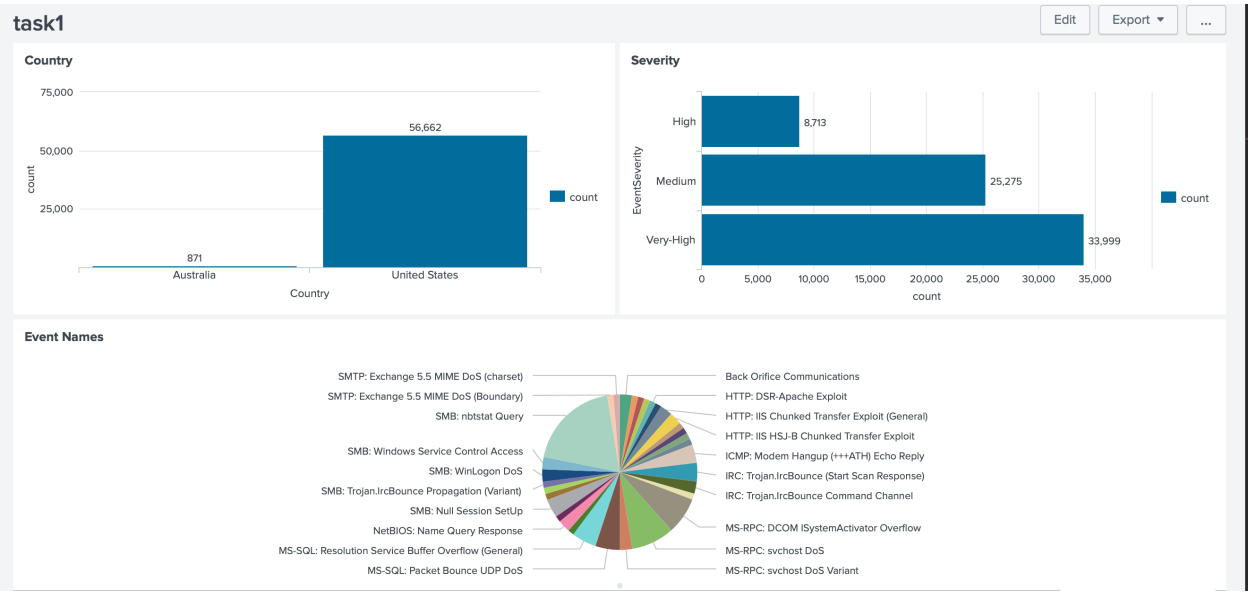
Events (67,987) Patterns **Statistics (39)** Visualization

20 Per Page | Format | Preview | Prev 1 2 Next

src	dst	Country	City	EventName	EventSeverity	count
1.1.1.1	216.136.107.136	Australia		ISAKMP: Windows 2000 DoS	Very-High	871
209.126.247.134	216.136.107.91	United States		IRC: Trojan.IrcBounce Command Channel	Very-High	1742
216.136.107.136	216.136.107.233	United States	Katy	FTP: Login with 'wh00t' Password	Medium	871
216.136.107.136	216.136.107.3	United States	Katy	SMB: Null Session SetUp	Medium	871
216.136.107.148	216.136.107.233	United States	Katy	HTTP: DSR-Apache Exploit	High	872
216.136.107.2	216.136.107.136	United States	Katy	NetBIOS: Name Query Response	Medium	1742
216.136.107.233	172.16.5.157	United States	Katy	FPSE: _vti_pvt/service.cnf Access	Medium	871
216.136.107.233	172.16.5.157	United States	Katy	HTTP: Apache2.pl Exploit	High	871
216.136.107.233	172.16.5.157	United States	Katy	HTTP: IIS %25%35%63 Double Encoded in URI	Very-High	871
216.136.107.233	172.16.5.157	United States	Katy	HTTP: dbmlparser.exe Access	Medium	871
216.136.107.233	172.16.5.157	United States	Katy	MS-SQL: Resolution Service Buffer Overflow (General)	Very-High	3484
216.136.107.233	172.16.5.157	United States	Katy	MS-SQL: Slammer-Sapphire Worm	Very-High	871
216.136.107.233	216.136.107.136	United States	Katy	HTTP: Null HTTP Server Heap Overflow	Very-High	872

*Sonuçların tamamı ekran görüntüsünde verilmemiştir.

IPS sisteminden alınan loglar üzerinde yapılan incelemede, seviyesi “Very High”, “High” ve “Medium” olarak belirtilen 39 kaydın 1 tanesi hariç geri kalanların United States kaynaklı olduğu tespit edilmiştir.



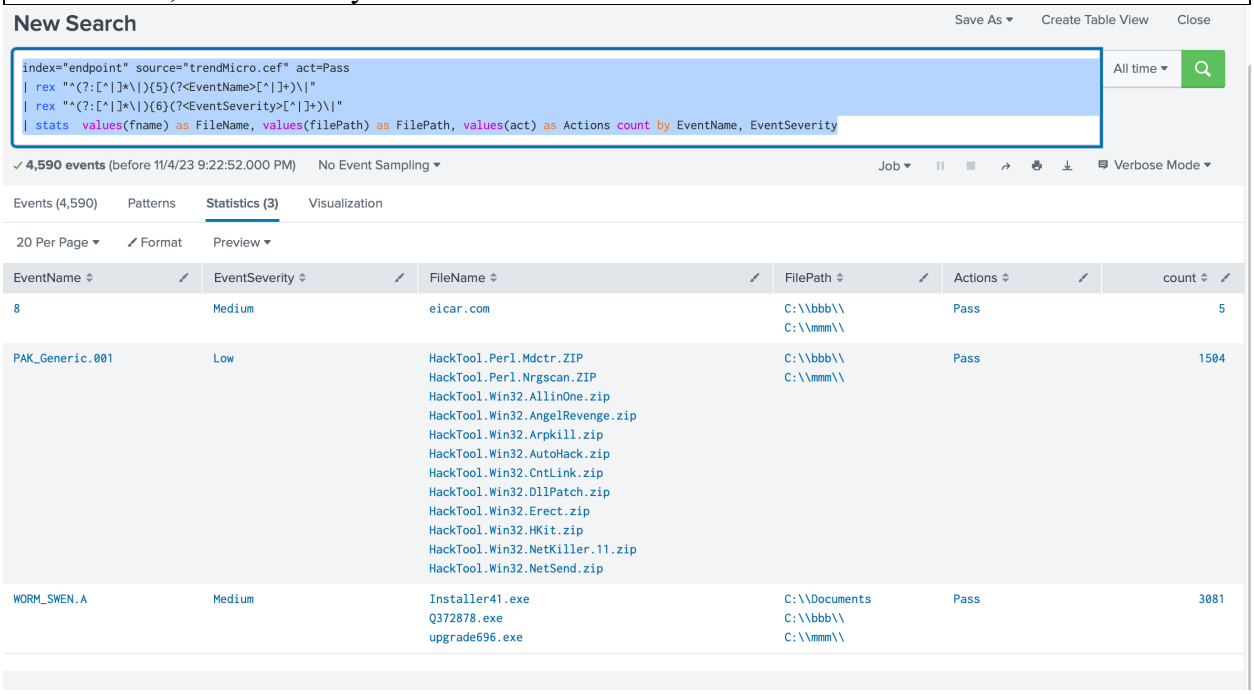
Bulunan bulgulara ilişkin olarak yukarıda görülen dashboard oluşturulmuş ve kaydedilmiştir. Kurumu hesefleyen malware ve event typeları buradan arz edilebilir.

Task 2 : We would like to create custom alerts, but we need help identifying the potential malware signatures and indicators of compromise. Specifically, I'm looking for the field names that might contain relevant information to find meaningful insights. "Trend Micro" antivirus software runs automatically, but what can be inferred from this? Could you elaborate on the functioning of EDR and AV in generating distinct signatures and their variations?

Kötü amaçlı yazılım imzaları ve iocleri oluşturmada antivirüs ve EDR çözümlerinden sağlanan bilgileri kullanmak önem arz etmektedir.
Antivirüs açısından dosya adı, dosya yolu ve dosyanın hash bilgisi, sistem dosyalarında yaptığı değişiklik yada bilinen imzalar ile karşılaştırılması önem taşırken edr'a yönelik olarak bakıldığında zararlının processleri, parent-child ilişkileri, ulşamaya çalıştığı ip ve domain isimleri, oluşturduğu registry kayıtları ve memory analizi ile daha çok davranışsal özellikleri girecektir.
Elimizde bulunan antivirüs sistemi olduğundan loglar incelendiğinde dosya isim ve yollarına ulaşabildiğinden aşağıdaki sorgu oluşturulmuştur. Action olarak pass seçilerek alan daraltılmaya çalışılmıştır.

Splunk Sorgusu:

```
index="endpoint" source="trendMicro.cef" act=Pass
| rex "^(?:[^|]*\|){5}(?<EventName>[^|]+)\|"
| rex "^(?:[^|]*\|){6}(?<EventSeverity>[^|]+)\|"
| stats  values(fname) as FileName, values(filePath) as FilePath, values(act) as Actions count by EventName, EventSeverity
```



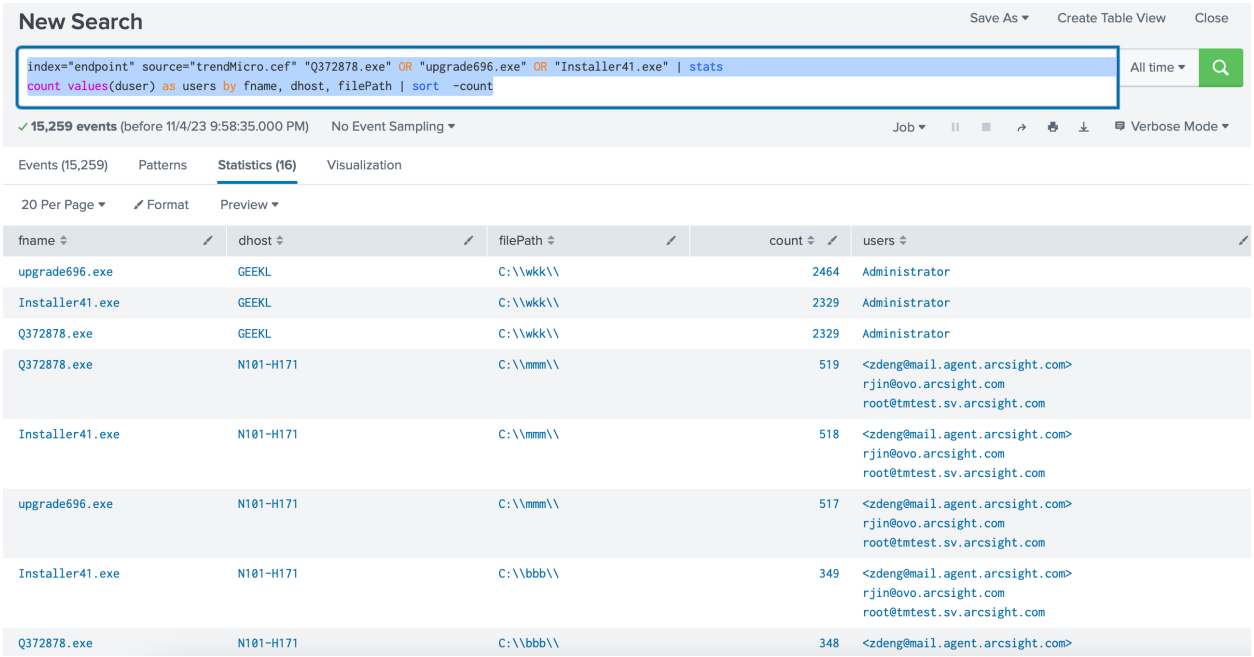
EventName	EventSeverity	FileName	FilePath	Actions	count
8	Medium	eicar.com	C:\\bbb\\ C:\\mmm\\	Pass	5
PAK_Generic.001	Low	HackTool.Perl.Mdctr.ZIP HackTool.Perl.Nrgscan.ZIP HackTool.Win32.AllinOne.zip HackTool.Win32.AngelRevenge.zip HackTool.Win32.Arpkill.zip HackTool.Win32.AutoHack.zip HackTool.Win32.CntLink.zip HackTool.Win32.DllPatch.zip HackTool.Win32.Erect.zip HackTool.Win32.HKit.zip HackTool.Win32.NetKiller.11.zip HackTool.Win32.NetSend.zip	C:\\bbb\\ C:\\mmm\\	Pass	1504
WORM_SWEN.A	Medium	Installer41.exe Q372878.exe upgrade696.exe	C:\\Documents C:\\bbb\\ C:\\mmm\\	Pass	3081

Buradan bulunan dosya isimleri ve yollarına yönelik olarak custom alert üretilmesi mümkündür. Burada özellikle Installer41.exe, Q372878.exe ve upgrade696.exe dosyaları dikkat çekmiştir.

Task 3 : It would also be advantageous to present the malware outbreak status from Trend Micro's product to HQ. Before investigating a potential malware outbreak, it is important to provide a brief explanation of malware and its behavior, such as how it spreads and distributes itself. It appears that one of our users' computers may be infected with malware. Looking at different hosts with the same malware signature can help you identify malware outbreaks.

Aşağıdaki sorgu ile daha önceki tasklarda zararlı olabileceğini değerlendirdiğimiz çalıştırılabilir dosyaların hangi makinelerde hangi kullanıcılar tarafından ve hangi dizinlerde olduğuna bakılmıştır.

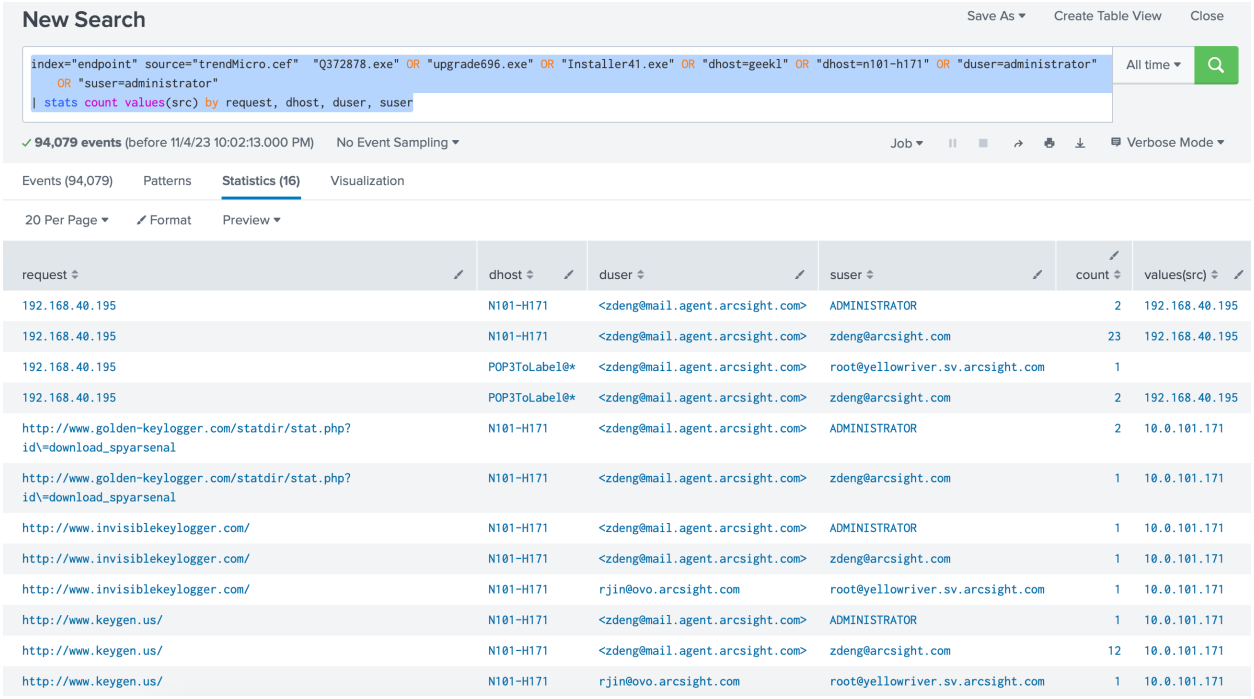
Splunk Sorgusu:
index="endpoint" source="trendMicro.cef" "Q372878.exe" OR "upgrade696.exe" OR "Installer41.exe" | stats count values(duser) as users by fname, dhost, filePath | sort -count



fname	dhost	filePath	count	users
upgrade696.exe	GEEKL	C:\\wkk\\	2464	Administrator
Installer41.exe	GEEKL	C:\\wkk\\	2329	Administrator
Q372878.exe	GEEKL	C:\\wkk\\	2329	Administrator
Q372878.exe	N101-H171	C:\\mmm\\	519	<zdeng@mail.agent.arcsight.com> rjin@ovo.arcsight.com root@tmtest.sv.arcsight.com
Installer41.exe	N101-H171	C:\\mmm\\	518	<zdeng@mail.agent.arcsight.com> rjin@ovo.arcsight.com root@tmtest.sv.arcsight.com
upgrade696.exe	N101-H171	C:\\mmm\\	517	<zdeng@mail.agent.arcsight.com> rjin@ovo.arcsight.com root@tmtest.sv.arcsight.com
Installer41.exe	N101-H171	C:\\bbb\\	349	<zdeng@mail.agent.arcsight.com> rjin@ovo.arcsight.com root@tmtest.sv.arcsight.com
Q372878.exe	N101-H171	C:\\bbb\\	348	<zdeng@mail.agent.arcsight.com>

Zararlı URL adreslerine ilgili kullanıcılar tarafından bir trafik olduğuna dair gözlem bulunmaktadır.

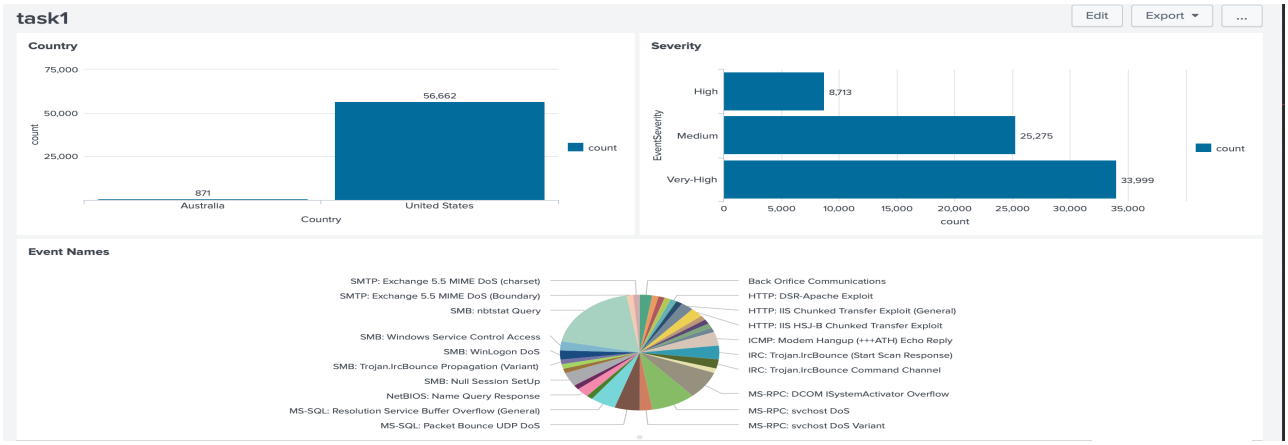
Splunk Sorgusu:
index="endpoint" source="trendMicro.cef" "Q372878.exe" OR "upgrade696.exe" OR "Installer41.exe" OR "dhost=geekl" OR "dhost=n101-h171" OR "duser=administrator" OR "suser=administrator" | stats count values(src) by request, dhost, duser, suser



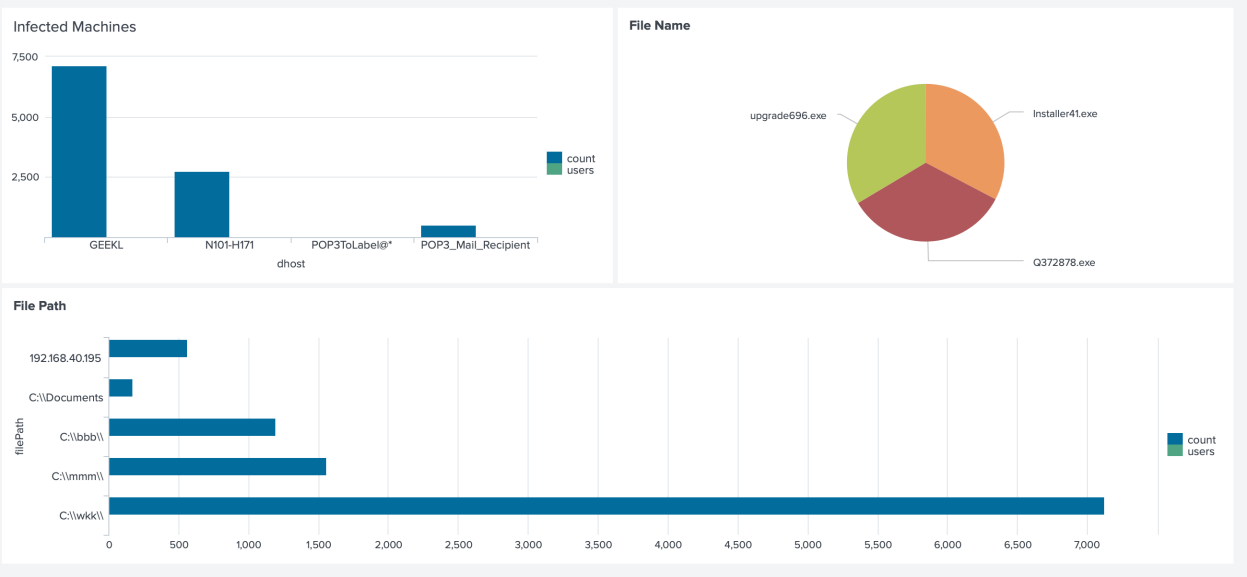
ANAMERKEZ İÇİN

Malicious Software yani kısaca malware kötü amaçlı yazılım anlamına gelmektedir. Cihazlara, ağlara ve verilere zarar vermek veya başka amaçlar için silmek, kaçırmak gibi amaçlarla tasarlanmışlardır. Elektronik posta ekleri, enfekte olmuş web siteleri veya yazılımların zafiyetlerini kullanalarak yayılabilirler. Bir sisteme girdiğinde, veri çalma, veri içeriğini bozma yada değiştirme, saldırgan için sisteme izinsiz giriş hakkı vermek gibi kötü amaçlı eylemler gerçekleştirebilir. Worm yada virüs gibi kendilerini çoğaltma ve diğer sistemlere yayılma ve zarar vermeye devam etme yetenekleri bulunmaktadır.

Daha önce oluşturduğumuz tasklarda ki genel tablo ile kuruma gelen saldırılar hakkında bilgi verilebilir.



Ayrıca zararlı ile ilgili olarak oluşturulan dashboard üzerinden bulgular genel olarak paylaşılabilir.



***Please remember that our headquarters team lacks technical knowledge, so your responses should include explanations. Avoid using a highly technical or documentation-style approach. Instead, create a report that includes Splunk search queries, along with relevant dashboard/panel screenshots, to clearly illustrate the answers to our questions. Submit your responses in PDF format.

Note: Use the index "endpoint".