

**CYBER STRUGGLE**

**TASK- SECURING THE MOTHERLAND**

**Hazırlayan:**

**DCS001 Hakan ŞEN**

**Ekim 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.

Tipping point İPS için CEF HEader Bilgilerini incelediğimizde ve açık kaynaktan yapılan araştırmada

CEF:<Version>|<Vendor>|<Product>|<Version>|<Signature\_ID>|<Name>|<Severity>|<Extension>

CEF:1|TippingPoint|UnityOne|<Version>|<Signature\_ID>|<Name>|<Severity>|<Extension>

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?

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.

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".