**----------------------------------------------------START OF TICKET----------------------------------------------------**

**Reporting Analyst(s):**

**Executive Summary: Provide a brief “story-like” narrative of the Incident. Include items such as:**

**• Reported Date/Time**

**• Incident Threat Title**

**• Any actions you take**

**o Assigned To**

**o Urgency**

**o Investigation of Multiple Incidents Created (Include Name of Investigation)**

**o Disposition**

**• OSINT information**

**Splunk Short ID:**

**Splunk Incident Link(s):**

**-------------------------------------------------------------------------------------------------------------------------------**

**Incident Review Information (from ESS Dashboard)**

**Risk Object:**

**Risk Score:**

**Risk Events:**

**Type:**

**Disposition:**

**Security Domain:**

**Urgency:**

**Status:**

**-------------------------------------------------------------------------------------------------------------------------------**

**Incident Information (after expanding the Incident)**

**Description:**

**This section is discretionary. Each type of incident in Splunk ESS has its own unique set of:**

**[a] Additional Fields and Field Values**

**[b] Event Details**

**[c] Information found in the raw data**

**[d] Information found in the Notable Response**

**[e] Information found in the Risk Analysis Response**

**[f] Information found in the logs**

**Include any host and user information as well as any source and destination IP address information in this**

**section. Basically, this section is where most of your artifacts and IOCs will be placed as well.**

**----------------------------------------------------------OSINT INFORMATION-----------------------------------------------------------**

**Malicious File(s)**

**Malicious File # 1:**

**• File Name:**

**• File Hash(es):**

**• VirusTotal Link:**

**o Risk Score:**

**• Other OSINT Resources:**

**Malicious File # 2:**

**• File Name:**

**• File Hash(es):**

**• VirusTotal Link:**

**o Risk Score:**

**• Other OSINT Resources:**

**IP Address(es) Reputation**

**IP Address # 1:**

**• VirusTotal Link:**

**o Risk Score:**

**• AbuseIPDB Link:**

**o Number of Times reported:**

**o Confidence of Abuse:**

**• URLScan.io Link:**

**o Verdict:**

**• Other OSINT Resources:**

**IP Address # 2:**

**• VirusTotal Link:**

**o Risk Score:**

**• AbuseIPDB Link:**

**o Number of Times reported:**

**o Confidence of Abuse:**

**• URLScan.io Link:**

**o Verdict:**

**• Other OSINT Resources:**

**Malicious URLs (Defanged)**

**Malicious Link # 1:**

**• VirusTotal Link:**

**o Risk Score:**

**• Other OSINT Resources:**

**Malicious Link # 2:**

**• VirusTotal Link:**

**o Risk Score:**

**• Other OSINT Resources:**

**-------------------------------------------------------------------------------------------------------------------------------**

**Additional Information:**

**-------------------------------------------------------------------------------------------------------------------------------**

**Declaration:**

**-------------------------------------------------------------------------------------------------------------------------------**

**Recommendations**

**Block IP Address(es):**

**Block URL(s):**

**Block Hash(es):**

**Credentials Reset:**

**------------------------------------------------------END OF TICKET-----------------------------------------------------**

**Notes to Reporting Analysts from CNL:**

**[1] Enhance your Jira tickets and reports by adding pictures and screenshots when applicable.**

**[2] An example of ‘Additional Information’ could be an explanation of the type of malware VirusTotal found in**

**a file attachment. If VT found Mimikatz malware then explain what that is so your readers will understand the**

**danger involved.**

**[3] Splunk ESS Incidents sometimes are about related incidents that originate from other CNL tools such as**

**Proofpoint and CrowdStrike. When doing a Splunk ESS Incident of this type you must include a full report about**

**the original incident from PP or CS in your Splunk ESS report also (all on one Jira ticket).**