Cisco: Umbrella Investigate

Cisco Umbrella Investigate provides internet-wide visibility of attacker’s infrastructure, predictive intelligence to identify malicious domains, IPs, and ASNs, and all the real-time and historical domain information you need in a single source. With the Splunk Add-on for Cisco Umbrella Investigate, you can automatically enrich security events inside Splunk with Cisco’s intelligence on domains, IPs, and networks across the internet. By leveraging Investigate’s threat intelligence from within Splunk Enterprise Security, you can gain more context about a domain, IP, or ASN related to the event, allowing you to make faster, more informed decisions when responding to critical incidents and researching potential threats.

Configuration

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). Refer to the documentation and the following:

- Add-on or app: Cisco Umbrella Investigate Add-on
- Cisco documentation: Umbrella Investigate Add-On for Splunk

Application

When your Splunk deployment is ingesting Cisco Umbrella Investigate data, you can use the data to achieve the following:

- Enriching suspicious email domains