

## EAS 596 - CYBERSECURITY ANALYTICS

### ASSIGNMENT 03

#### GROUP- 5:

Ayyathurai Jaya, Raghavi Preeti

Heeb, Collin

Kandasamy, Kathiresan

Patnayakuni, Sharada

Pindi, Naren

**1) Describe what an IOC is, give an example of where you could get an IOC, and then list out three ways in which you would use an IOC as a Security Analyst in your day-to-day operations with Splunk.**

An **IOC (Indicator of Compromise)** is a piece of forensic data that identifies potentially malicious activity on a system or network. IOCs can include **IP addresses, domain names, URLs, file hashes, email addresses, or registry keys that indicate a cyberattack.**

**Example Source of IOC: AlienVault OTX**, which provides real-time threat intelligence from open-source feeds.

#### **Three ways to use IOCs in Splunk:**

- ✓ **Threat Hunting:** Use IOCs to proactively search through logs for signs of compromise using queries.
- ✓ **Alerting:** Set up real-time alerts that trigger when an IOC matches live data, such as detecting communication with malicious domain.
- ✓ **Correlation Searches:** Link IOCs with other log sources (firewall, DNS, endpoint logs) to identify lateral movement or multi-staged attacks.

**2) Create a search where you would map out the IP address based on the country where it came from. See below for an example diagram. There is no need to include a screenshot or detail how to make the graph, just give the query. In addition, what value do you see in this mapping technique? Give 3 use cases where you think creating a map like this would prove to be valuable in an organization (think outside of this dataset).**

#### **QUERY:**

```
index="homework_3"  
| iplocation ip  
| stats count by Country  
| geom geo_countries featureIdField=Country
```

**Advantage of Mapping Technique:** Mapping IP addresses by country helps quickly visualize the geographical distribution of network traffic. This enables security teams and analysts to identify unusual patterns or potential threats based on location.

#### Use Cases:

- ✓ Mapping Technique helps to identify **unusual spikes** in traffic or attacks originating from unexpected countries (e.g., a sudden flood of login attempts from a high-risk region).
- ✓ **Access Policy Enforcement:** Useful for enforcing **geo-based** access control policies - e.g., blocking or alerting when access is attempted from countries where the organization does not operate.
- ✓ It also helps **marketing** or **operations teams** understand where users are connecting from, supporting business decisions like content localization, server placement, or product demand forecasting.

**3) Create two additional searches based on the data in the index and for each, describe why you see value in these searches and how it could be used in a Splunk diagram to provide security value.**

#### QUERY:

```
index="homework_3"
| stats count by type
| sort -count
```

#### OUTPUT:

| type   | count |
|--------|-------|
| url    | 6571  |
| ip     | 2414  |
| sha256 | 498   |
| domain | 398   |
| md5    | 119   |

This search helps identify the most frequently observed types of **Indicators of Compromise (IOCs)** such as **url**, **ip**, **sha256**, **domain**, and **md5**. Knowing which types are most common allows security teams to focus detection and mitigation strategies accordingly.

For example, if **URL IOCs** dominate, the organization might tighten web filtering rules or invest more in phishing detection. A bar chart visualization would provide a clear snapshot of IOC distribution, guiding incident response priorities.

QUERY:

```
index="homework_3"
| stats count by user
| sort -count
```

OUTPUT:

| user ↕          | count ↕ |
|-----------------|---------|
| ecarlesi        | 2101    |
| AP_Zenmashi     | 1886    |
| KesaGataMe0     | 1581    |
| drb_ra          | 806     |
| pingineer_jp    | 597     |
| HeliosCert      | 546     |
| malwrhunterteam | 265     |
| PhishStats      | 159     |
| harugasumi      | 148     |
| phishunt_io     | 142     |
| dubstard        | 98      |
| kubotaa3        | 92      |
| CardanoPhishing | 71      |
| DonPasci        | 65      |
| MalwarePatrol   | 57      |
| JAMESWT_MHT     | 56      |
| RdpSnitch       | 55      |
| illegalFawn     | 54      |
| 500mk500        | 53      |
| 1ZRR4H          | 48      |
| CsirtPost       | 47      |
| dnstwist        | 44      |
| ozuma5119       | 43      |
| idclickthat     | 41      |
| Max_Mal_        | 40      |

This search identifies which users are associated with the most IOC hits. This could reveal specific individuals being targeted by phishing or malware campaigns. High counts on a particular user may suggest a compromised account or elevated risk requiring investigation.

This can be visualized in a column chart or table to assist SOC analysts in proactively defending high-risk user accounts, implementing additional monitoring, or triggering password resets if necessary.