NIST SP 800-53 incident response

You would like to achieve an organization-wide perspective on incident awareness and response by correlating incident information and individual incident responses. This will help with compliance to NIST SP 800-53 rev5.

Required data

- Data normalized to the following Common Information Models:
  - Intrusion Detection
  - Malware

To optimize the searches shown below, you should specify an index and a time range.

Intrusion detection

Unique sources of external intrusion attempts

To see the locations from where intrusion attempts on your system occur, run the following search.

```
| tstats count FROM datamodel=Intrusion_Detection.IDS_Attacks WHERE nodename=IDS_Attacks.Network_IDS_Attacks AND (IDS_Attacks.src="*") BY IDS_Attacks.src IDS_Attacks.category IDS_Attacks.action IDS_Attacks.signature
| stats count BY IDS_Attacks.src
| iplocation IDS_Attacks.src
| geostats count BY Country
```

Count of anomalies detected by IDS signature

To get a count of events calculated to have a high probability of being anomalies, run the following search.

```
| tstats count FROM datamodel=Intrusion_Detection.IDS_Attacks WHERE nodename=IDS_Attacks.Network_IDS_Attacks AND (IDS_Attacks.signature="*") BY IDS_Attacks.signature anomalydetection count
| stats count
```

You can also see this information in a table with the count for each signature by using the following search instead.

```
| tstats count FROM datamodel=Intrusion_Detection.IDS_Attacks WHERE nodename=IDS_Attacks.Network_IDS_Attacks AND (IDS_Attacks.signature="*") BY IDS_Attacks.signature anomalydetection count
| rename IDS_Attacks.signature AS Signature count AS "Event Count"
| table Signature "Event Count"
```
### Attack categories observed

To get a count of the attack categories observed on your systems, run the following search.

```splunk
| tstats count FROM datamodel=Intrusion_Detection.IDS_Attacks WHERE nodename=IDS_Attacks.Network_IDS_Attacks AND (IDS_Attacks.category="*") BY IDS_Attacks.category
| chart sum(count) BY IDS_Attacks.category
| sort -count
```

### Malware detection and protection

#### Hosts with multiple infections

To get a list of hosts that have more than one malware infection, run the following search. You can change the `sum_signatures > 1` argument to a value greater than one if needed.

```splunk
| tstats dc(Malware_Attacks.signature) FROM datamodel=Malware WHERE (Malware_Attacks.signature="*") AND (Malware_Attacks.dest="*") BY Malware_Attacks.dest
| rename Malware_Attacks.dest AS dest dc(Malware_Attacks.signature) AS sum_signatures
| eval multi_infections = if(sum_signatures > 1, 1, 0)
| stats sum(multi_infections)
| rename sum(multi_infections) AS Endpoints
```

#### Trend in malware attacks

To see how many malware attacks hit your system over time, run the following search. You can change the `span` to a value other than one second.

```splunk
| tstats count FROM datamodel=Malware WHERE (Malware_Attacks.signature="*") BY _time Malware_Attacks.signature span=1s
| timechart sum(count) BY Malware_Attacks.signature useother=0
| fillnull value=0
```

#### Trend in malware protection actions

To see how many malware protective actions your system took over time, run the following search. You can change the `span` to a value other than one second.

```splunk
| tstats count FROM datamodel=Malware WHERE (Malware_Attacks.action="*") BY _time Malware_Attacks.action span=1s
| timechart sum(count) BY Malware_Attacks.action useother=0 usenull=0
| fillnull value=0
```
Next steps

After running these access controls and taking appropriate action, you may want to look into other NIST SP 800-53 rev5 controls:

- Access control
- Audit and accountability
- Configuration management
- Identification and authentication
- Risk assessment
- System and information integrity

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.