DevOpsSchool
Lets Learn, Share & Practice DevOps

Elastic SIEM Essentials Training

Curriculum 3 Days

E

- **SIEM Introduction**
- **SIEM Components**
- **Setup and Configure ELK**
- **Understanding a types of Threats**
- **Introduction to threat hunting on an endpoint platform**
- **Hunt types**
- **Install Beats shippers**
    ○
    ○
    ○
    ○
- **Data Source in ELK for Security Scanning**

E

- **Enable modules and configuration options**
- **Auditbeat & Discover Anomaly detection**
  - **System module - Linux, macOS, Win**
    -
    -
    -
    -
    -
  - **Auditd module (Linux Kernel Audit info)**
  - **File integrity module (FIM) - Linux, macOS, Win**
- **Filebeat & Discover Anomaly detection**
  -
  -

- **Winlogbeat & Discover Anomaly detection**
  -
- **Packetbeat & Discover Anomaly detection**
  -
  - E
  -
- **Filebeat & Discover Anomaly detection**
  -
  - E
  -
  - E
  -
  -
  -

E

- **Understanding SIEM UI**
  - ○
  - ○
  - ○
  - ○ S E
- **Threat Hunting with Kibana**
  - ○
  - ○
  - ○
  - ○ E
  - ○
  - ○
- **Elastic Endpoint Security Triage and Response**
  - ○
  - ○
  - ○ E
  - ○
  - ○