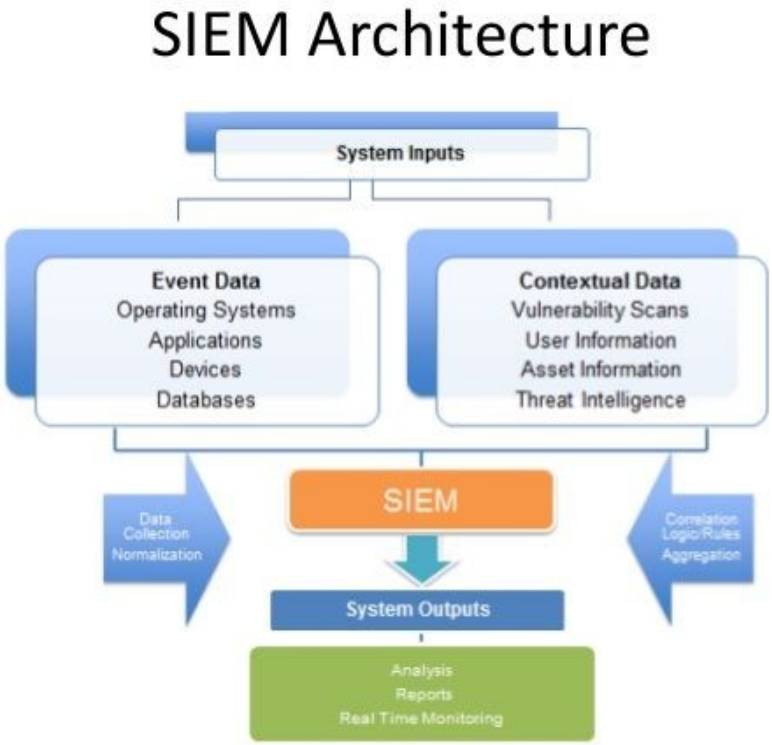


Intro to Wazuh

What is Wazuh?

- Open source XDR & SIEM
- Security Information Event Manager
- Collects data from many machines
- Parses that data into searchable events
- Real-time alerting based on that data



Why use Wazuh?

Why Use Wazuh?

- Easy to set up compared to other tools
  - Simple, cross platform agent
  - Single, one-liner installer
  - Easy to use dashboard
- More efficient blue-team operations
  - Frees up people from watching logs
  - Automatically maps vulnerabilities
  - Real-time alerting

Exercise: Deploy Wazuh

Exercise: Deploy Wazuh

- Get into groups of 3
- Each group will deploy one Wazuh Indexer/Dashboard stack and two Agents (on three separate machines)
- Once the indexer/dashboard stack is running, navigate to the web UI
- Create an alert that reports all incoming and outgoing ssh connections to all of the endpoints

documentation.wazuh.com