SAND2019-8544D

Splunk/Airwatch Integration

Charles Carrington, North Carolina A&T State University

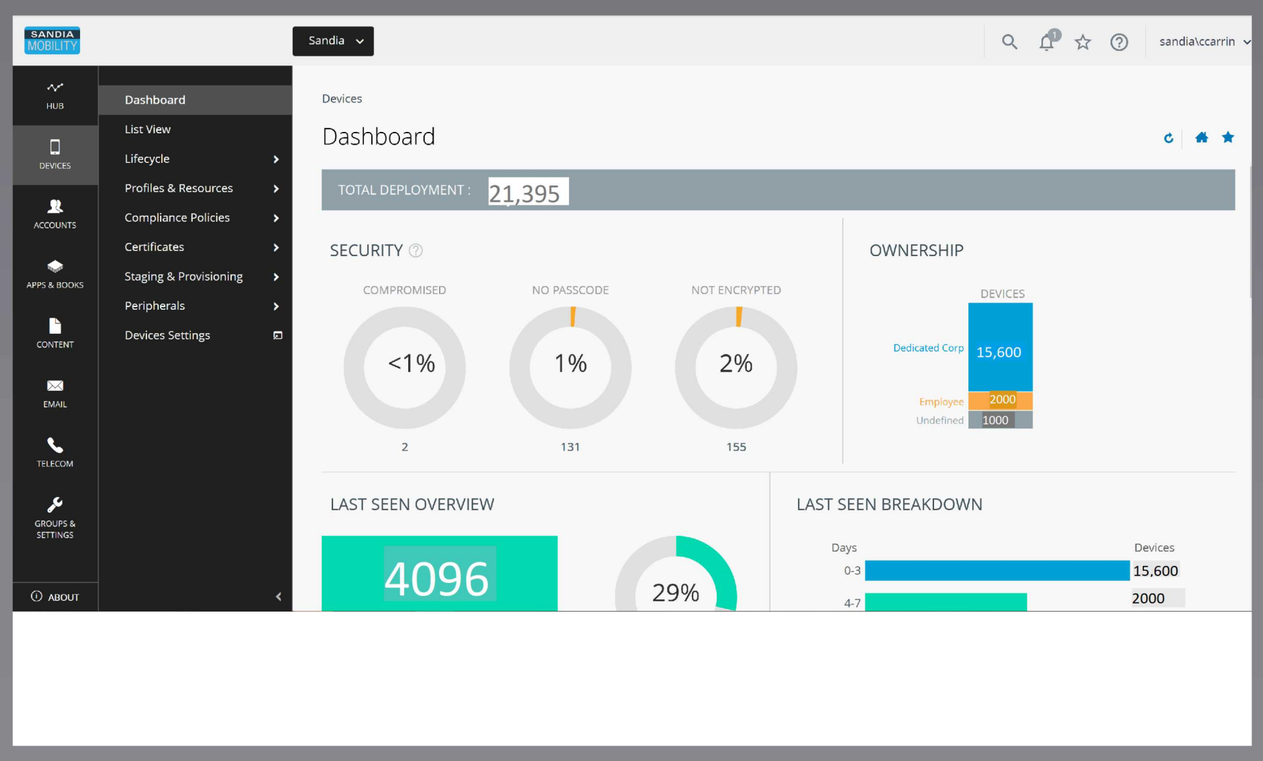
Project leads: Elizabeth Walkup 09312, Jonathan Mandeville 09317

Problem Statement

Sandia, like many companies, has business phones (iPhones/Android) that are used by employees. These phones are managed and monitored with AirWatch/OneWorkspace. However, our incident response team works mainly in Splunk, a logging aggregation platform that does not have any good integration with AirWatch. We want to give the incident response team better visibility into AirWatch in Splunk.

Objectives & Approach

- Setup Splunk forwarder for sending data in to Sandia Splunk Enterprise instance
- Determine useable AirWatch API endpoints and begin sending the data to Splunk.



Technical Challenges

- There is no widely available suitable medium between the Splunk and AirWatch System.
- Configurations have to be created in Splunk to recognize JSON format returned from calls to AirWatch API endpoints

End Goal

Splunk will allow the IR team to do more efficient threat hunting and set up alerts in real-time

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2019-???????