The Center for Cyber Defenders
Expanding computer security knowledge

SAND2018-7374D

OSINT Integration Tool

Tiffany Chiang, UC Berkeley
Caroline Kish, Georgia Institute of Technology

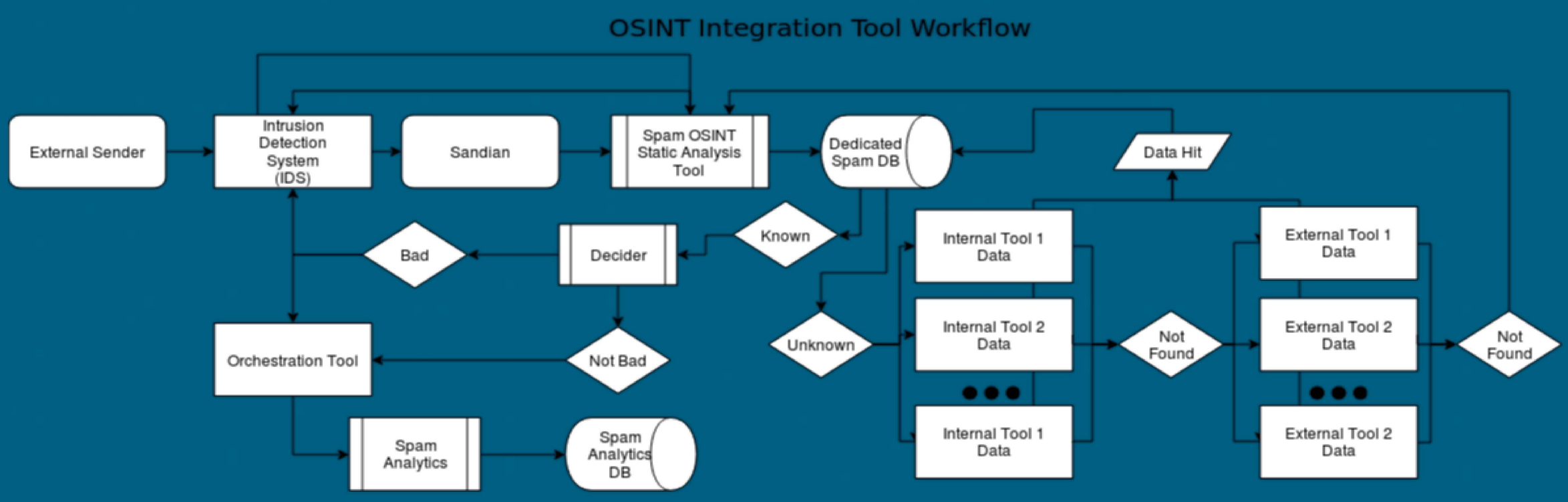
Seanmichael Galvin (9312) and Wellington Lee (9312)

PROBLEM STATEMENT

Identifying spam and phishing emails is a difficult task even with intrusion detection systems. The difficulty for machines and humans is that no malicious emails are alike, and most are tailored to look close, if not identical, to benign emails. Our tool leverages the potential link between the human and machines' abilities to identify suspicious material, each approaching the identification problem from a different perspective. While our tool checks the email against internal and Open Source Intelligence (OSINT) data, we also rely on Sandians as remote sensors in our IDS to flag suspicious emails.

APPROACH

1. Explore different data sources (internal and external OSINT), and write modules to incorporate these into Sandia's existing internal email analysis tool.
2. Use the results obtained from internal and OSINT tools to automatically classify emails.
3. Provide feedback to reporter on email and optionally enact some action.
4. Analyze the data to better determine how to protect Sandia from phishing attacks and emails containing dangerous malware.



IMPACT AND BENEFITS

This tool improves Sandian workflow in two distinct spheres: response analytics and education of workforce. With the module, we can keep track of spam/phish reports and even their accuracy, useful statistics in determining Sandia's vulnerabilities. We are also able to provide feedback to members of the workforce who submit emails to the spam inbox, allowing for more interaction on the reporter's side. The module will also free up the IR team's time from processing the inbox to work on more important and urgent tasks.

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. SAND2017-XXXXC.