Event Sentry Documentation

Release latest

Aug 29, 2019

Contents:

Release: latest

Event Sentry automatically manages ACE events and incidents and seeks to automate most of the common tasks performed by an intel analyst.

CHAPTER 1

Major Features

- **Generates comprehensive wiki write-ups** to give analysts deep insight into the event.
- **Detects types of malware** using built-in and extendable detection modules.
- **Detects kill chain phase** by determining if a user clicked a link, submitted credentials, opened a malware sample, etc.
- **Extracts indicators** from e-mails, sandbox reports, and other artifacts.
- **Automatically uploads indicators** to SIP and creates appropriate relationships between them.
- **Maintains an event repository** containing copies of the ACE alerts and all their artifacts.
- **Creates a shareable intel package** containing a summary of the event including indicators, malware samples, and e-mail headers.

CHAPTER 2

Compatibility

Event Sentry has been tested with the following configurations:

- Ubuntu 14.04 with Python 3.4
- Ubuntu 18.04 with Python 3.6

2.1 Required

Event Sentry currently requires the following systems:

- ACE
- SIP
- Confluence

2.2 Recommended

The following systems are technically optional, but they are highly recommended in order to realize the full potential of Event Sentry:

- Splunk
- Carbon Black

CHAPTER 3

Installation

Event Sentry provides an installer script to help get you up and running. It will ask where you would like it to be installed and will install all dependencies inside of a virtual environment.

```
git clone https://github.com/IntegralDefense/eventsentry.git
cd eventsentry
./installer.sh
```

After running the installer script, it will notify you of the various config files you must edit and how to run the provided unit tests to ensure things are configured properly.

3.1 User Guide

Blah

3.2 Developer Guide

Blah