**PROJECT SYNOPSIS**

**By Harleen Kaur(Student of Btech CSE at GTBIT)**

**Title :** Development of a tool for Application Whitelisting on any PC/Server using OSQUERY Framework+

**Start date :** 6th June 2019

**Expected completion date :** 31st July 2019

**Objective :** To develop a tool to query any Operating System for system attributes and leveraging it to impose an application whitelisting function in order to secure the endpoints providing assurance that no illegitimate applications are allowed to run.

**Drivers for this Project:**

Almost all Cyber Security research reports of recent times (2018-19) has found that more than 250000 new samples of malware are created daily and that number will continue to grow in the future.

A majority of those are undetectable during the first few hours since it’s release to the wild. Some will even elude detection for longer periods.

However, the point of the matter is that in those undetected hours, considerable damage may have already dealt by these “Zero-day” attacks.

With advanced threats like ransomware causing so much irreparable damage in such a short time, merely relying on the reactive approach of blacklisting may not be the most sensible solution. The main reason is that antiviruses let anything run as long as they aren’t considered a threat. The basic objective of Zero-day malware is to run undetected.

As such there is an acute requirement of Application Whitelisting to secure the organizations. By incorporating Application Whitelisting, zero-day malware will always be blocked given the nature of such files being freshly created and almost guaranteed not found on an existing whitelist. Even the most dangerous malware can do nothing if it’s not allowed to run.

An application whitelist is a list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a host according to a well-defined baseline. The technologies used to apply application whitelists—to control which applications are permitted to install or execute on a host—are called whitelisting programs, application control programs, or application whitelisting technologies. Application whitelisting technologies are intended to stop the execution of malware and other unauthorized software. Unlike security technologies such as antivirus software, which block known bad activity and permit all other, application whitelisting technologies are designed to permit known good activity and block all other.

**Scope:**

All the Endpoints in an IT infrastructure to be covered with centralized management.

**Requirement Specifications:**

* To Ensure that all the Endpoints are having Application whitelisting enabled and no illegitimate application/process is allowed to run
* To provide a centralized dashboard for generating alerts on the illegitimate process/application tried to run
* To manage the application whitelistings including exceptions through same centralized dashboard.

**Solution Proposed:**

The solution is designed with following approach:

1. Open Source OSQUERY Framework+ (OSQUERY d/ OSQUERY CTL) to be installed on a Central Server
2. Integration with host systems having different Operating Systems will be done
3. Information from different systems will be collected in database
4. Using OSQUERY Extension and Python – to develop a functionality to disallow execution of non-whitelisted application

**Technichal Details:**

* Installing OSQUERY d and OSQUERY CTL on UBUNTU
* Python and Python development tools
* MYSQL

**Usefulness:**

The project derives its ultimate benefit in zero day protection and in monitoring of the real time system state.

**Current Status:**

* Conceptualized

**Timelines:**

* Conceptualization and Project synopsis 🡪 10th June 2019 ; 24th June 2019
* Set up OSQUERY Framework 🡪 18th June 2019 ; 26th June 2019
* Pilot integration of Hosts 🡪 24th June 2019; 30th June 2019
* Development of Centralized dashboard 🡪 30th June 2019; 2nd June 2019
* Development and integration of

Python functions for use-cases 🡪 10th July 2019; 5th July 2019

* Solution UAT 🡪 15th July 2019
* Solution Pilot testing 🡪 20th July 2019
* Solution Pilot rollout 🡪 25th July 2019

**Market Potential:**

Monitoring of System state/attributes is essential for any Cyber Security product and as such various organizations are looking at these types of solutions which gives granular controls on the applications and processes.

**Last word and future development :**

The solution is powerful and has potential of extending it to integrate with various security technologies to provide automated responses on complex IOCs (Indicators of compromise).