Launch Report - Cycle 3

For

FreeEDR

Submitted by

FreeEDR

|  |  |
| --- | --- |
| **Instructor:** | Professor Greg Hislop |
| **Team Members:** | Bryan Bolesta, Ryan Fiers, Declan Kelly, Matthew Horger, Layla  Phills, Zachary Santoro, Marisa Tranchitella |
| **Cycle:** | 3 |
| **Date Submitted:** | 3/15/2020 |

Document Template copyright 2005-2019, Gregory W. Hislop. Version 2.2. Use permitted under Creative Commons license CC-BY-NC-SA. See http://creativecommons.org/licenses/by-nc-sa/3.0/.

Grading Rubric - Launch Report - Cycle 2

This rubric outlines the grading criteria for this document. Note that the criteria represent a plan for grading. Change is possible, especially given the dynamic nature of this course. Any change will be applied consistently for the entire class.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Achievement** | **Minimal** | **Exemplary** | **Pts** | **Score** |
| **Content** | Section(s) missing, not useful, inconsistent, or wrong. | Provides all relevant information correctly and with appropriate detail |  |  |
| Post Mortem |  |  | 40 |  |
| Plan |  |  | 30 |  |
| **Grammar and Spelling** | Many serious mistakes in grammar or spelling | Grammar, punctuation, and spelling all correct | 10 |  |
| **Expression** | Hard to follow or poor word choices | Clear and concise. A pleasure to read | 10 |  |
| **Tone** | Tone not appropriate for technical writing | Tone is consistently professional |  |  |
| **Organization** | Information difficult to locate | All information is easy to find and important points stand out | 10 |  |
| **Layout** | Layout is inconsistent, visually distracting, or hinders use | Layout is attractive, consistent, and helps guide the reader |  |  |
| **Late Submission** |  |  |  |  |
| **Total** |  |  | 100 |  |

Launch Report - Cycle 3

This report documents the launch of a new project cycle. It includes a post mortem of the cycle just completed, and basic elements of a plan for the cycle being launched.

**Post Mortem for Cycle 2**

## Summary

Based on the Launch Cycle 2, the team met and accomplished all four objectives. MS Planner was established as the main work tracking system and mostly maintained week to week. For the majority of deliverables, the documents or tasks were completed with enough time to UAT acceptance and final product integration. Clear communication was maintained among the team members as well as with the faculty advisor and stakeholder. The following continued development of the project implementation was completed:

* The FreeEDR Outlook MailService and API was successfully built-out and tested using the [freeEDR@outlook.com](mailto:freeEDR@outlook.com) address.
* Each page of the Dashboard was initialized with each component that will be included in the final implementation, but only populated with test data.
* A full testing suite for each internal API made entirely in Postman was created.
* Approximately 70 unique Sigma detection rules were added to the rule repository, 16 of which were developed from scratch for this project.
* Core FreeEDR script functions were developed and implemented such as the ability to install Python, retrieve Sigma rules from the repository, retrieve rule updates, and the ability to read and write Custom Windows events
* Process and Network forensic APIs were researched for compatibility with our project and chosen based on their capabilities. Functions were developed and implemented to allow for interaction and data retrieval from the VirusTotal and Hybrid-Analysis APIs.

## 

## Issues

**Issue**: Scheduling Issues

**Solution**: Utilization of voice/video communication system (Discord, texting/call), working remotely, regularly scheduled remote working sessions, utilization of collaboration software/systems (Google Drive, GitHub)

**Issue**: Project Documentation and Cycle Deliverables Work Last Minute

**Solution**: Project Manager being more on top of the team to get the work done on internally set dates to allow for enough buffer time to review documents before submission

**Issue**: Coronavirus Changes

**Solution**: Due to the coronavirus affecting other’s work schedules outside of senior design, our presentation for the final had to be changed to fit the new video requirements.

**Plan for Cycle 3**

## Objectives

The team’s objectives for this cycle are:

* Dashboard
  + Produce a variety of API-generated reports that are able to be printable for our final presentation
  + Integrate the XML Parser into the Dashboard via API calls to make the dashboard function properly without test data
  + Create a custom authorization server with roles and claims for each of the FreeEDR team members and advisors so they are able to only access certain parts of the dashboard
  + Move the Dashboard and API onto the same VPC as the FreeEDR Domain
* Infrastructure
  + Consolidate and unify the functions within the main FreeEDR script
  + Plan and execute simulated attacks against test workstations to evaluate the integrity of the Sigma detection rules and the efficiency of the FreeEDR script
  + Set up direct link between FreeEDR script and dashboard

## Project Support

|  |  |
| --- | --- |
| Version control | Github repository access has been granted to instructor here: <https://github.com/mhorger3/FreeEDR> |
| Document repository | Documents will be stored on Git, but collaborative work will again take place on Google Drive: <https://drive.google.com/drive/folders/108JcpIo5g1oQHi4NEEmKi_l9MR-kO4XO?usp=sharing> |
| Tracker(s) | Team tasks are tracked using Microsoft Planner, which instructor has access to here: <https://tasks.office.com/drexel0.onmicrosoft.com/en-US/Home/Planner/#/plantaskboard?groupId=d2cc81b1-9066-4d32-8e1f-d5a8aa77bd23&planId=TDG8edQdYUCGTTJi1XEtpmQAGbWB> |
| Product Summary | Website has been submitted |

## Activities

The table below shows the initially identified set of activities for this cycle and assigns a lead person to each activity.

|  |  |  |
| --- | --- | --- |
| **Week** | **Person** | **Contribution** |
| 1 | MH | Produce First Batch of Reports |
| 2 | MT  ZS | Finish Requirements Document  Complete Integration between script and Dashboard |
| 3 | MH  ZS | Integrate XML Parser into Dashboard  Identify Requirements for Environment Testing |
| 4 | MT  ZS | Finish Design Document  Create Sigma Rules to Identify Environment Testing |
| 5 | Everyone | Midterms |
| 6 | MH  ZS | Finish Custom Roles for Dashboard  Complete Endpoint Threat Visualizations |
| 7 | ZS  ZS  ZS | Complete Environment Testing  Finish Documentation for Script Deployment  Complete Demo for Script Deployment |
| 8 | MH MT  Everyone | Finish Complete Dashboard on FreeEDR Domain  Finish End of Project Poster  Complete CCI Showcase |
| 9 | MT | Finish Implementation Document |
| 10 | Everyone | Finals |

## 

## Team Members Key

|  |  |
| --- | --- |
| **Name** | **Initials** |
| Bryan Bolesta | bb |
| Ryan Fiers | rf |
| Declan Kelly | dk |
| Matthew Horger | mh |
| Layla Phills | lp |
| Zachary Santoro | zs |
| Marisa Tranchitella | mt |