Polaris Sight RESEARCH & DESIGN

March 22, 2018

Version 1.0

STUDENTS

|  |  |
| --- | --- |
| Student Number | Group Member Name |
| N9152237 | Curtis Dooley |
| N8962375 | Owen Charters |
| N10115307 | Rui Lin |
| N94748511 | Peijun Xue |

## Research and Design Documentation

This section of our project consists of an analysis of similar products and a survey with relevant individuals that would be interested in our product. Additionally, initial designs for what our product will look like are planned supported once user stories have been finalised. Regarding our survey; an Incident response team has been contacted that would be available to review our initial plans for the product.

The aim of this research will be to identify:

* Analysis of similar products
* Survey of relevant customers
* A list of optimal open source incident response tools
* Designs and functionality that fulfil use cases

The outcomes of the research will be fully incorporated into the design.

|  |  |  |
| --- | --- | --- |
| Story ID | Story Title | Story Points |
| 1 | Elicitation, Requirement Analysis and Project Scoping |  |
| 2 | Analysis of market and similar products |  |
| 3 | Revenue model |  |
| 4 | Formal literature review |  |
| 5 | Survey of customers |  |
| 6 | Creation of holistic view of the product; project management, report and presentation |  |
|  | Story Point Sub-Total: |  |

**Delivery Schedule**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Week 8 | Week 9 | Week 10 | Week 11 | Week 12 | Week 13 |
| Sprint 1 | | Sprint 2 | | Sprint 3 | |
| Release 1 | | | | | |

**Competitor Analysis**

The competitor analysis for our product has been restricted to the following:

* Is the competitor open source?
* Was the tool designed for incident response?
* Does the tool have multiple functionality?

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Incident Response Tool | Ease of Use | Open Source | Multiple OS | Actively Maintained | Data Breach Identification |
| GRR Rapid Response | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) |  |
| CimSweep |  | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) |  |  |  |
| CIRTkit |  | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) |  |  |  |
| Kolide | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) |  |
| MozDef | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) |  |
| TheHive | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) |  | [Image result for green tick](https://www.google.com.au/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjdn_CIif7ZAhVCFJQKHe-vCHwQjRx6BAgAEAU&url=http://www.i2clipart.com/clipart-green-tick-28a8&psig=AOvVaw237gYnaseZmmQ4aF-qv7BV&ust=1521744094444794) |  |

**Survey of Relevant Customers**

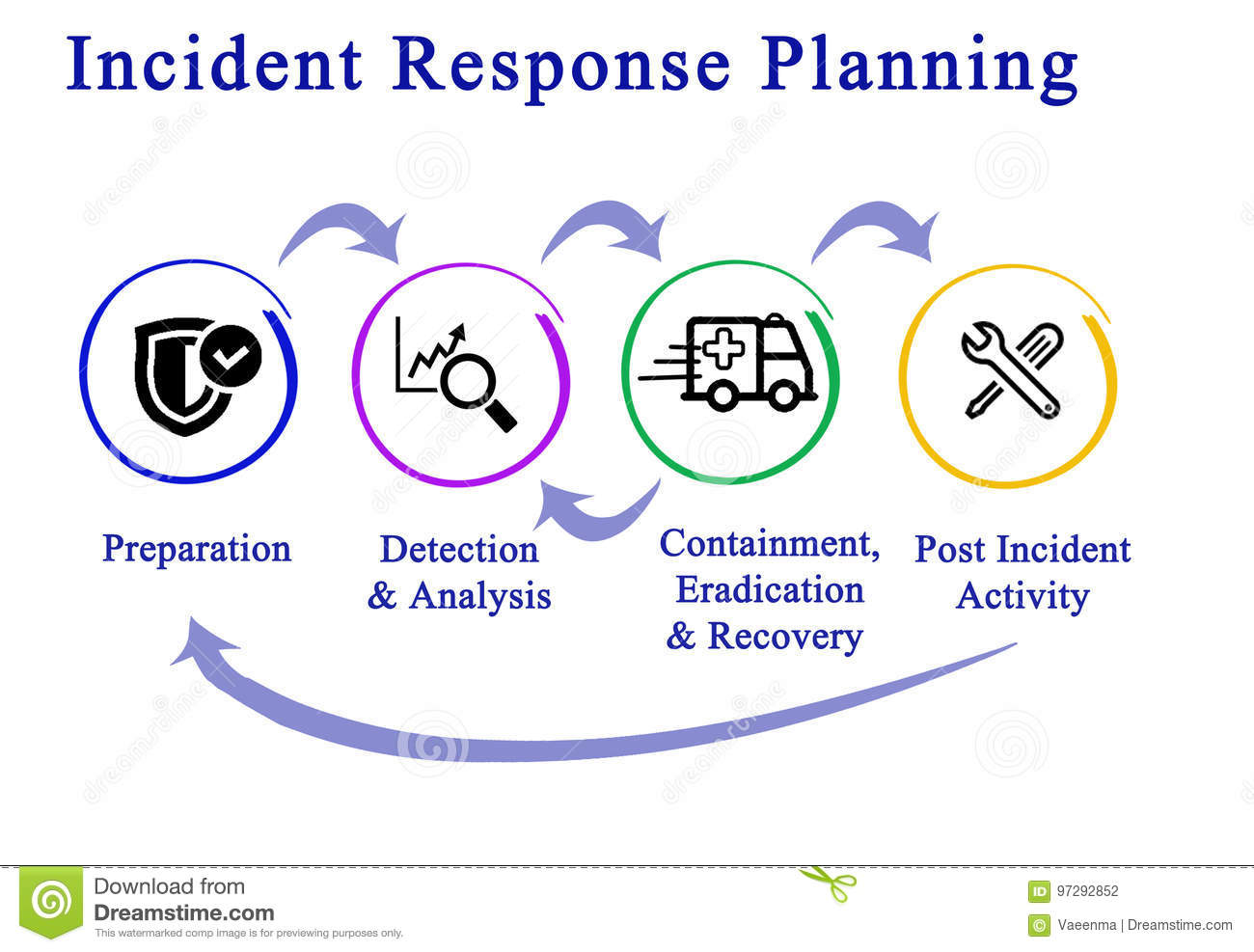
(Pending)

Additional information and designs are required.

Contact with Incident Response team is available when these requirements are met.

**Incident Response Life Cycle – Relevant Tools**

A list of possible tools that could improve our incident response tool has been collected. These tools have been selected keeping in mind what is involved in an incident response. Below is a typical life cycle diagram used to demonstrate how an incident response works.



**Detection & Analysis**

**Evidence Collection**

[bulk\_extractor](https://github.com/simsong/bulk_extractor) - bulk\_extractor is a computer forensics tool that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures. Because of ignoring the file system structure, the program distinguishes itself in terms of speed and thoroughness.

Status: Open Source | Supports: Windows, Linux & OS X

**Incident Management**

[FIR](https://github.com/certsocietegenerale/FIR/) - Fast Incident Response (FIR) is an cybersecurity incident management platform designed with agility and speed in mind. It allows for easy creation, tracking, and reporting of cybersecurity incidents and is useful for CSIRTs, CERTs and SOCs alike.

Status: Open Source | Supports: Windows, Linux & OS X

**Log Analysis Tool**

[Lorg](https://github.com/jensvoid/lorg) - a tool for advanced HTTPD logfile security analysis and forensics. Useful for websites that have been compromised.

Status: Open Source

**Sandboxing**

[Virustotal](https://www.virustotal.com/) - Virustotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners

**Attributes of Compromise:**

Domains

* **High**
  + Same Actor Controlled 2nd-level
* **Medium**
  + Watering Hole
  + Compromised
* **Low**
  + Same Dynamic DNS Provider
  + Network Comms

IP Addresses

* **High**
  + Domain Resolutions
* **Medium** 
  + IPv4 Address
  + Server IP Port Combination
* **Low**
  + Same Netblock

Email

* **High**
  + Actor-Owned Email
* **Medium**
  + Spear-Phishing Sender
  + Domain Registrant Email
* **Low**
  + Phishing target

Malware

* **High**
  + Same Compile Time
  + Custom Tool, in use by one group
* **Medium**
  + Unique Strings
  + Mutex
* **Low**
  + Publicly Available Tool
  + Tool Author

Victim

* **High**
  + Same computer / host
* **Medium**
  + Same compromised account
* **Low**
  + Same victim organisation

Methodology

* **High**
  + Registry Key change
* **Medium**
  + Unique Password or File path
* **Low**
  + Overall methodology