

Project Plan

Cyberthreat Insight Discovery & Visualization Tool

Webroot

Prepared by CU Boulder Capstone Team

October 10, 2019

1. 5. Project Plan

1. Development Stack

- The team plans to develop the interface as a web app similar to current industry products like Virus Total.
- Project architecture plans include using the following libraries/languages:
 - Node.js for communication between the database and web app
 - React for frontend UI design
 - An AWS NoSQL database to store IoC database
- Which AWS solution we choose will depend on cost analysis
- A JavaScript graph visualization library to construct the IoC relationships
- The framework we choose will be included in the project proposal

2. Schedule

Project Phase:	Deliverables/Milestone:	Baseline Time Box Dates (Subject to Change)	
<u>Initiate</u>	<ul style="list-style-type: none"> ● Designate time(s) for weekly team meetings ● Meet with Webroot primary contacts & establish meeting schedule ● Study project background ● Assign team roles ● Establish project budget ● Initiate project 	Start	Finish
		9/16/19	10/11
<u>Plan</u>	<ul style="list-style-type: none"> ● Complete Project Charter ● Develop rough development cycle <ul style="list-style-type: none"> ○ Define technologies ○ Define container/component architectures ● Submit (to Webroot) a project proposal ● Familiarize with chosen tech stack ● Develop detailed development cycle & finalize technologies ● Develop work (schedule) 	Start	Finish
		10/14	12/13
<u>Execute</u>	<ul style="list-style-type: none"> ● Finalize detailed requirements ● Complete API support <ul style="list-style-type: none"> ○ Authenticated access to Threat Analysis Pipeline database ○ Query of artifacts ○ Compound IoC queries 	Start	Finish
		12/16/20	4/24/20

Project Plan – Cyberthreat Insight Discovery & Visualization Tool

	<ul style="list-style-type: none"> ○ Unit tests ● Complete User Interface Support ○ Display of queried Artifact metadata ○ Display of queried IoC data ○ User creation of graph nodes ○ Vector linking of graph nodes (based on correlating queries) ● Complete API + Database support ○ Storage of user created node graphs ○ Retrieval of user created node graphs ○ Storage of user defined tags ○ Sharing of node graphs between users ○ Unit Tests ● Complete testing 		
<u>Close</u>	<ul style="list-style-type: none"> ● Final test cases ● Ensure final deliverable meets predetermined requirements ● Receive approval to close project 	Start	Finish
		4/27/20	5/11/20