Dell Inc is a large enterprise level organization, with an ecommerce platform (www.dell.com) that serves millions of people annually. As such, Dell is a globally known brand. Due to this, people that visit and shop with Dell expect a high degree of quality and trust in service. Quality refers to the user experience while visiting the site, including ease of use and being provided with relevant, useful content. Trust is the users being provided with what they were promised, as well as making sure their information is not used for purposes other than those they've been notified of.

In the e-commerce space, payment information is one the most sensitive pieces of data that a user trusts a retail provider with. Thus it is the responsibility of retail providers to not only make sure that they only use the data as authorized by the user, but also to ensure that the data is protected, so that malicious actors do not steal their data, and potentially commit fraud with the information.

Dell has strict policies that dictate how sensitive information like this is handled. Dell also has numerous ways to ensure that a users information is secure, and safe from attack.

Recently, however, there have been breaches in online retailers that haven't been seen before. More information can be found online by searching for breaches by magecart on British Airways, Newegg and TicketMaster. This attack circumvents a lot of existing security approaches, and seems to be a new way of stealing user information. With something as sensitive and serious as payment information, it is always better to be proactive than to respond after the problem occurs. Hence, we here at Dell Inc. are looking for ways to secure our users data against this and similar attacks.

The project being proposed for the capstone team requires the team to come up with potential approaches to handle this; by trying to prevent the breaches from happening, detect the breaches (either attempted or successful), and act if a breach happens (either attempted or successful).

Over the course of this project, the team will approach problem solving in a more self-starter, innovative fashion as opposed to strictly directed fashion. They will analyze and propose multiple solutions to smaller sub problems iteratively.

The team will also be encouraged to increase their own understanding of the problem, including things like the impact and the clients needs and concerns.

At the end of the project, the deliverable needs to include implemented code and possibly a (or multiple) process to handle these breaches. A stretch goal is to make the code and process scalable and modular, so as to include other possible security concerns in the future.