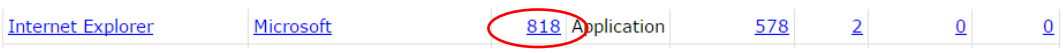
# Teacher Summary: *Product Analysis*

This document provides instructor guidelines for one of the ten integrated curriculum projects developed for the NSF-funded Necessary Skills Now (NSN) project (award #1501990). The NSN project partners consist of CORD and three national centers supported through the NSF's Advanced Technological Education (ATE) program: National Center for Systems Security and Information Assurance (CSSIA), Florida Advanced Technological Education Center (FLATE), and South Carolina Advanced Technological Education National Resource Center (SC ATE). The NSN project is designed to integrate employability skills into technical exercises, activities, and labs. The project partners created self-contained instructional modules vertically aligned to associate degree programs in **mechatronics/automation in manufacturing** and **cybersecurity in information technology**. (The activities described in this document support courses in cybersecurity.) Six categories of employability skills, repeatedly mentioned in workforce surveys and research reports, served as the focus of the integrated curriculum:


This project addresses the skills highlighted above.

| Faculty Resources | |
|---|---|
| **Section** | **Content** |
| **Project Overview** | The purpose of this project is to incorporate employability skills (teamwork, problem-solving, verbal and written communication skills) into an exercise that focuses on exposing students to using the proper resources to make product selection recommendations.<br><br>Courses for Implementation: Security+<br><br>Key Terms: vulnerabilities, CVE, product selection, product recommendation |
| **Discussion** | Cybersecurity professionals must be familiar with the CVE Details website, the interface to Common Vulnerabilities and Exposures, the dictionary of publicly known cybersecurity vulnerabilities. The information provided at the CVE Details website can be used to help an individual analyze and evaluate various products and technologies.<br><br>**The Scenario:**<br>Acme Corporation has recently experienced cyber-attacks and data breaches that have resulted in a significant financial loss and a loss of consumer confidence. Acme hired a new chief information security officer. The CISO informed the cybersecurity staff that the organization will undergo a comprehensive threat analysis and begin to collect data to establish purchasing and deployment standards. The CISO wants to ensure that the organization uses empirical data in selecting products and establishing of standards in lieu of opinions of staff members or a sales pitch from vendors.<br><br>Over the last decade, the federal government and other organizations collected substantial data regarding product vulnerabilities and flaws. This data is freely available to organizations interested in performing product analysis. The Common Vulnerability Exploit (CVE) database is one example of a national resource available to cybersecurity professionals used to perform product analysis. The CVE Details website allows individuals to perform a deep analysis in comparing technologies.<br><br>After several incident response investigations, it is apparent that many attacks were the result of browser and email vulnerabilities. The CISO has tasked the cybersecurity staff with analyzing the organization's Internet browsers. The investigations identified that over 95% of all users employ one of four browsers: Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, and Microsoft Edge. |
| **Objectives** | Student Learning Objectives (Career and Technical, employability, etc.)<br><br>a. ***Technical*** – Each team will analyze the vulnerabilities of three products.<br><br>b. ***Verbal Communication*** – Each team is required to successfully and efficiently communicate among themselves using proper terminology, and create a PowerPoint presentation that successfully communicates their analysis.<br><br>c. ***Problem Solving*** – Teams must successfully collect data and analyze the vulnerabilities associated with the products given in the scenario. A recommendation will be made based on those results.<br><br>d. ***Teamwork*** – Students will demonstrate the ability to work in teams to analyze the vulnerabilities of the scenario products and make a recommendation based on empirical data.<br><br>e. ***Written Communication*** – Teams must demonstrate the ability to summarize the data collected in the form of Excel spreadsheets using charts and tables. |

| Faculty Resources | |
|---|---|
| **Section** | **Content** |
| **Teaching Strategies** | Step 1 – Review the project and objectives with the class. Introduce *Common Vulnerabilities Exposures*—the catalog of known security threats sponsored by the United States Department of Homeland Security (DHS), divided into two categories: vulnerabilities and exposures. Students can refer to the CVE website, specifically About CVE, for a good summary. (10 minutes)<br><br>Step 2 – Watch the videos Cybersecurity Taxonomy (14:43) and Top 50 Security vulnerabilities by products in 2015 (7:52)<br><br>Step 3 – Discuss the various types of vulnerabilities and vulnerability classification. (15 minutes)<br><br>Step 4 – Review the Roles and Responsibilities section 2 (pp 4–5) of the NIST publication NIST Guide to Selecting Information Technology Security Products. (10 minutes)<br><br>Step 5 – Form three-person teams of students. Distribute copies of ***3_Student_ProductAnalysis*** document. Teams discuss and complete their research and write a summary report. Give a time limit (e.g., 30 minutes) for creating 7–10 minute presentations.<br><br>Step 6 – Each team delivers their presentation to the class. |
| **Student/Group Activity Steps** | 1. Review the project and objectives. (10 minutes)<br>2. Watch the videos as a class. (25 minutes)<br>3. Form and gather members of teams, as directed by instructor.<br>4. Following the instructions in ***3_Student_ProductAnalysis,*** each team completes a two-page summary report (45 mins) and a PowerPoint presentation (30 minutes).<br>5. Each team will deliver their presentation to the class (7–10 minutes). |
| **Expected/Result and Solutions** | 1. Students working in teams will demonstrate the use of industry tools to compile empirical data used to establish organization standards and drive product selection.<br>2. Each team will complete a two-page written report supported by tables and charts.<br>3. The team's recommendation will be supported by the team's gathered data.<br><br>Answers will vary since the data on the CVE Details site changes. To find the data at the CVE Details website:<br><br>• Select Browse > Products from the menu along the left-hand side of the page.<br>• To find Google Chrome, for example, select "C," and scroll (or jump) through the pages until you find the Product Name for "Chrome." Select the link under "# of CVE Entries" to research the list (sometimes hundreds!) of security vulnerabilities for this product.<br><br>  <br>Chrome Google 1 OS 2 0 0 0<br>Chrome Google 1357 Application 971 278 0 1<br>Chrome Techland 1 Application 0 0 0 0<br><br>• Or, for Microsoft Internet Explorer, select "I," and advance through the pages to find the Product Name for "Internet Explorer." Select the link under "# of CVE Entries."<br><br>  <br>Internet Explorer Microsoft 818 Application 578 2 0 0<br><br>• Or, for Mozilla Firefox, select "F," and advance through the pages to find the Product Name for "Firefox" by "Mozilla." Select the link under "# of CVE Entries."<br><br>  <br>Firefox Mozilla 1437 Application 1661 1078 0 2<br><br>And so forth, for other products. You may choose to extend this activity by assigning a similar activity to investigate other types of products, such as word processors (e.g., Microsoft Word, |

| Faculty Resources | |
|---|---|
| **Section** | **Content** |
| | Word Perfect, TextMaker, Google Docs), email (Microsoft Outlook, Mozilla Thunderbird, Google Gmail, Opera), and so forth.<br>4. Presentations by each team need to be short and quick, yet engage all members of the team. See the *Verbal Communications Rubric* for advice to achieve an excellent score. |
| **Equipment** | Computer with Internet access |
| **Faculty Resources** | |
| **Background Materials** | 1. Websites:<br>a. Common Vulnerabilities and Exposures<br>b. NIST Guide to Selecting Information Technology Security Products<br>c. CVE Details |
| **Student Handouts** | • ***3_Student_ProductAnalysis*** |
| **Assessment** | Assess student performance and abilities by referring to the compilation of rubrics in **4_Rubric_ProductAnalysis** for<br>• Teamwork Rubric<br>• Problem Solving Rubric<br>• Verbal Communication Rubric<br>• Written Communication Rubric<br>• Technical Rubric |