Following are the questions for your Case Study. Your response expectations are outlined per question. Your reading is Radware-2022-Global-Threat-Analysis-Report from https://www.radware.com/getattachment/b775fe9c-326f-4f97-b6c7-8545b5b68e42/Radware-2022-Global-Threat-Analysis-Report.pdf.aspx , the 2023 Data Breach Investigations Report by Verizon https://www.verizon.com/business/resources/T47b/reports/2023-data-breach-investigations-report-dbir.pdf and the https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf These reports are in the files section. <mark>Do not restrict yourself to these reports in your quest for answers</mark>. Use tables, figures, and diagrams, if needed, to illustrate your answers. A cover page with your name, class/section and collaborators is required. A final page of references is also required. While collaboration is encouraged, your responses and submissions are individual. Ensure the use of your own words for your responses. The quality of your submission is expected to be semi-professional at a minimum. Submission file should in .pdf and named <Lastname_CS7349_CaseStudy>. Please maintain the same font and font size of the questions when writing your answers. There is no limitation on references.

1. What are the main differences AND similarities between the above two reports? Note that the two companies are in different domains, but both are in the business of Enterprise Security. Please outline your responses CLEARLY, in your own words, in a MINIMUM of 1 page, with a MINIMUM of 5 differences and 3 similarities. This will help you compare and contrast multiple cybersecurity reports. Your responses need to be in the technical and business domains. E.g. "a difference between the two reports is one report is from 2022-2023, and the other report from 2023" OR "Radware report is 37 pages, while the Verizon DBIR is 89 pages", or similar responses on the format, appearance, length and design of the report will incur zero (0) marks. Cutting and pasting from the report, or other sources will result in a grade of zero.

2. In the reports, please identify 5 emerging Application Security trends for 2023. What was the business impact, and projected business impact of these trends? (business impact can include loss in $; loss in reputation; restructuring and new investments; executive departures, brand and reputation loss). A MINIMUM of 1 page is expected. This will help you look for business impact in general if you were a CIO or CSO, putting forth policies to mitigate loss. (Hint: External lookup may be necessary; take an example from each emerging trend and search for impact. A small paragraph per emerging trend+impact).

3. From the Verizon DBIR report, please summarize five (5) incidents, of <mark>different types</mark>, and their impact (e.g Do not give 2 DDoS incidents or 2 Supply Chain attack incidents. Provide 1 of each). These are specific attacks and their business impact. (a) what was the incident (b) how did the incident occur? (what vulnerability was exploited) (c) how was the vulnerability fixed (if at all, or if a fix was in place and not put in) (d) what was the impact? ($ loss, reputation, restructuring, etc). A MINIMUM of 1 page is expected. This will bring you up to speed on the top cybersecurity incidents of 2022. Your response must be clearly laid out (Hint: Use a table; do not restrict yourself to the reports. Responses should be numbered, with a) thru d) responses for each. Avoid single line responses).

4. What do the reports outline as next steps (mitigation approaches) for 2023. 3 approaches from Radware and 3 approaches from Verizon are requested. The goal is to compare the focus from 2 different companies, in different domains, looking at the same problem of how to secure IT in enterprises. A MINIMUM of 1 page is expected. Feel free to use other references.

5. What are the overall trends expected globally in 2024? Using the WEF Report, please identify 2024 a) 5 major trends b) give 2 examples for each trend. A MINIMUM of 2 pages is expected. Use external references wherever necessary to support your responses.