Analysis Document

In this project, we developed python scripts that automate system monitoring, network checks, and log analysis for our financial cybersecurity system. We used the data analytics process to collect, clean, and transform our data to be able to extract insights from it. Our data collection from the python script we created shows our source of logs, sensors, and user activity within the system. We cleaned the data and transformed it, fixing inconsistencies which further allowed us to extract insights. The insights we gathered allowed visualization of the system's security status, as well as algorithms to be applied to predict future security risks.

Our python scripts read and parsed log files to detect potential security incidents our system may have. They identified suspicious patterns within the logs, like unauthorized access and failed login attempts. The suspicious patterns found were then generated in a summary report text document named summary_report.txt. Nine suspicious logs were found. The report generated flagged the suspicious log incidents for further review.

Our python scripts also monitored the aspects of system performance by outputting memory and CPU usage. They collected performance metrics from the system at regular intervals using the psutil library, logged the performance data, and generated an alert via email when the performance threshold of CPU usage of 0.1% was met or exceeded. The percentage usage metrics were documented into a file named performance_log.txt for review.

Our python scripts implemented an effective automated alert generation system when the CPU usage was high by using the email API sendgrid and the smtplib library. The code sends an email to the specified email address of an employee to alert them that their CPU usage is high. Sending this email causes the employee to reduce their CPU usage by removing some of their files they may not need, for instance. In this way, the system will not exceed its threshold and fail.

Finally, our python scripts implemented an effective routine to scan for vulnerabilities and monitor network traffic. Nmap, the subprocess library, and scapy are in the automated code to run security checks. Scapy monitors the network traffic and nmap scans for vulnerabilities on the network. By using scapy in our code we can see the automation of collection and analysis of network traffic data, like packet counts. Our code captures 10 packets. By using nmap to scan for vulnerabilities, we can see through the report generated if the network is up or down.

While we had functional scripts and effective automation within our financial cybersecurity system, we had a challenge of data integration. It was difficult to find a log to

test and put into our code. We found a small dataset to process for the purposes of basic data analysis for this project. A bigger dataset would have also been a challenge to integrate because a high volume of financial data can be overwhelming to a system, needing more advanced tools and infrastructure. Since our system is of the financial sector, the data analysis process is very useful since it provides alerts to our employees and security teams when potential harm or threat is done. A trend in the financial sector of cybersecurity is that risks need to be identified and put out, if possible, immediately since money is involved. Based on our created python scripts and updated system diagram layout from our requirements given in an interview, our system is being built up from the ground up. The data in our system was previously poorly stored in a windows defender, anyone had access to the system, and employees were not properly trained. These were the three biggest problems in our system that needed addressing and have caused some risks and vulnerabilities in our system since it is now brand new.

Through data analysis, we have detected risks and vulnerabilities within our new system. Zero-day exploits will be common as there will be attacks on the system that will be unknown to fix at first. As with any new system there will be events training does not cover. Insider threats from our employees could also occur intentionally or unintentionally, but unintentional incidents are most likely. Employees can see the appointment times available in the database and take times from coworkers on a first come first served basis. DDoS attacks, overwhelming the system to disrupt services, are another thing our system is susceptible to since the system could have a lot of users trying to make the same appointment or do their tasks at the same time. Users would be back and forth between the appointment screens. Our company would take a big financial hit if it was down for a short period. As with other companies, data breaches and phishing are risks for their systems that are present in ours. According to our system diagrams, the active directory stores all of the login data, and the secure encrypted database stores all data for the company. If the active directory is down, there are still measures in place like MFA and the firewall that must be passed through for someone to login. Since there are three solid measures in place to get into the system, there is not a critical level for a data breach. There is still a high level for it though if MFA is bypassed. If MFA is bypassed identity theft and our company's financial data will be compromised. MFA in our system proves that a user is who they are, so without it users can more easily gain access to the system. Emails can also be sent from an outside source, as with any company system, because hackers want information. Systems admin, the internal security team, and the incident response team all need to be aware of the practice of phishing. Lastly, there is cloud vulnerability in our system. Transferring old data to the new database will make the data more secure for

employees to use and view. Misconfiguration of the data is what we have to watch out for while making this transfer.

Overall data analytics enhances financial cybersecurity systems by enabling threat detection, real-time monitoring, and risk management. The importance of incorporating data analytics into systems will only increase in future years.