**AI for Cyber Security – Project Proposal**

Team 9

**Section 1: Project Team Composition**

Team Member Bios:

**Chris Felkey (team coordinator)**: Chris is an IT professional with over 20 years of experience in Data Warehousing and Data Analytics. Currently, Chris serves as a Sr Manager within the Enterprise Data Office at Truist Bank where he manages the Shared Service BI Delivery organization which does reporting and analytics for every line of business at the bank. Previously Chris was a consultant working with clients in Financial Services, Oil and Gas and Consumer Packaged Goods on various business intelligence projects.

**Ahmed Mohamed Hassan**: Ahmed is an applications Manager for an investment company in the Middle East. Ahmed has an 17 years of experience in IT management and enterprise solutions in Oracle, SAP, and MS dynamics.

**Samjhana Lama**: Samjhana Lama is a business analyst, working for an international automotive solutions company. She has seven (7) years of experience in business as well as financial analysis, focusing on program profitability, business intelligence, business process improvement, financial projection/forecasting and system automation. Samjhana can contribute to this project with her experience in business strategy, analysis and business intelligence which will help in insightful and actionable reports for our AI4cyber platform.

**Section 2: Industry Selection and Background**

**Industry:** Financial Services

Financial Services covers a broad range of companies that provide both consumer and business offerings such as: Investment Banking, Credit Cards, Payments processing, Digital Banking, Insurance services and traditional retail or consumer banking.

The financial services industry is the driving force behind much of US and global industry, providing the funding needed for both large and small companies in addition to individual financial services people require like insurance and checking accounts. As of 2018, the industry accounted for 7.4% of the US gross domestic product and employed over 6.3 million people (*Financial services spotlight, n.d.*). The US banking sector had $17.4 trillion in assets in support of the worlds largest economy (*Financial services spotlight, n.d.*). The insurance sector had net premiums written on $1.1 trillion as of 2016 (citation). Another sector, Private Equity employs nearly 11.3 million people in the United States and 19.6 million worldwide (*Financial services spotlight, n.d.*). Us Based private equity firms have invested over $500 billion in the US alone in 2017 (*Financial services spotlight, n.d.*).

**Major Industry Players:** Visa, Mastercard, JP Morgan Chase, Bank of America, Allianz, AXA, Goldman Sachs, Morgan Stanly, Merril Lynch, Chase, Wells Fargo (*ictsd.org, n.d.)*

Technology has quickly become the backbone of how financial services companies operate. Mobile and Online banking have replaced in person trips to the bank for most people. This means technology to power the website or phone app, the technology to move money between accounts at different financial institutions as we use these services to pay bills. Investment banking firms utilize technology to connect the consumer to the markets and process trades on exchanges, in some cases replacing the person on the floor buying and selling shares in person. Communication between the customers and employees of the firms is now almost entirely digital. Regulatory reporting is now almost entirely digital.

**Section 3: Summary of Existing Threats Targeting Selected Industry**

Symantec Report reveals that in 2018, employees of small organizations were more likely to be hit by email threats—including spam, phishing, and email malware—than those in large organizations. We also found that spam levels continued to increase in 2018, as they have done every year since 2015, with 55 percent of emails received in 2018 being categorized as spam. Meanwhile, the email malware rate remained stable, while phishing levels declined, dropping from 1 in 2,995 emails in 2017, to 1 in 3,207 emails in 2018. The phishing rate has declined every year for the last four years.  
Also Symantec Reports saw fewer URLs used in malicious emails as attackers refocused on using malicious email attachments as a primary infection vector. The use of malicious URLs in emails had jumped to 12.3 percent in 2017, but it dropped back to 7.8 percent in 2018. Symantec telemetry shows that Microsoft Office users are the most at risk of falling victim to email-based malware, with Office  
files accounting for 48 percent of malicious email attachments, jumping from 5 percent in 2017.

In The finance industry malicious emails rating (1 In ) 491, Malicious URL 7.7 %, email phishing rating (1 iN) 2,628, email spam rating 56.7%

**Section 4: Existing AI4Cyber Platforms for Industry**

There are not a lot of industry specific solutions for the Financial Services industry. There are a lot of companies advertising their expertise with Financial Services organizations as the Financial Services sector is one of the most targeted because of the amount and type of data that a data breach would give access to.

One such company that is target the financial services sector is SenseOn, which advertises their threat detection and response platform which monitors an organizations network and deploys “Investigator Bots” to probe the organization from the inside and outside. SenseOn’s “AI Triangulation” is advertised as accurately flagging suspicious behavior so that the cyber security teams can further investigate while ignoring false alerts which would waste the security teams time. (SenseOn, n.d.)

DefenseStorm also offers a platform that uses machine learning to automate “cybersecurity and cybercompliance” for financial services firms. (Bharadwaj,2019)

Feedzai offers software that they claim helps banks and merchants detect and prevent money laundering. (Bharadwaj, 2019)

**Section 5: Relevant Data Sources**

Our plan is to focus on phishing and malware threats as these are some of the more prominent threats to financial services organizations. **PhishTank** is a great source of phishing information. The **Canadian Institute for Cybersecurity** has many datasets on malware threats. **Stratospehere IPS** and the **UNSW-NB15 Dataset** also provide malware data.

**Section 6: References**

*What are the largest financial services companies? – ictsd.org*. (n.d.). Retrieved March 13, 2022, from <https://www.ictsd.org/what-are-the-largest-financial-services-companies/>

*Financial services spotlight*. Financial Services Industry Spotlight | SelectUSA.gov. (n.d.). Retrieved March 13, 2022, from <https://www.selectusa.gov/financial-services-industry-united-states#:~:text=Financial%20markets%20in%20the%20United%20States%20are%20the,and%20indirect%20job%20creation%20in%20the%20United%20States>.

*Cyber security for financial services - AI threat detection*. SenseOn. (n.d.). Retrieved March 13, 2022, from <https://www.senseon.io/financial-services>

Bharadwaj, R. (2019, October 7). *AI for cybersecurity in finance - current applications*. Emerj Artificial Intelligence Research. Retrieved March 13, 2022, from <https://emerj.com/ai-sector-overviews/ai-cybersecurity-finance-current-applications/>

Symantc Internet Security Threat Report Volume 24 |Feberuary 2019 https://docs.broadcom.com/doc/istr-24-2019-en