CS668 Assignment – 2

Total Marks – 100
Submission Deadline – 26th Feb 2024

This is a group-based project. Each group will be assigned one report among the reports listed at the end of this document.

1. Here is what you will need to do:
    a. Read the report assigned to your group and map to ATT&CK tactics and techniques (as shown in Module 3.3)
    b. Use ATT&CK navigator tool to create a layer to store the mapping and use hyperlink facility to add additional contextual information for each technique as obtained from the report (As shown in Module 3.4)
    c. Save the layer into Excel format (As shown in Module 3.4)
    d. Document defensive Recommendations for all the techniques identified (as outlined in Module 3.5)

2. Create a single PDF file for each group with a cover page that mentions your group number, the names and roll numbers of group members with the following sections:
    a. Details of your approach to mapping finished reporting to ATT&CK
    b. The defensive recommendations with rationale
    c. References you used to reach the defensive recommendations
    d. Assumptions about the organization

3. The assignment of Reports is as follows:

Group Name	Assigned Report
G1	checkpoint-blindeagle.pdf
G2	blog-netlab-360-com.translate.goog-Be vigilant The modified CIA attack kit Hive enters the field of black and gray production.pdf
G3	blog.group-ib.com-Dark Pink.pdf
G4	trendmicro.com-Earth Bogle Campaigns Target the Middle East with Geopolitical Lures.pdf
G5	unit42.paloaltonetworks.com-Chinese Playful Taurus Activity in Iran.pdf
G6	qianxin-kasablanka.pdf
G7	trendmicro.com-New APT34 Malware Targets The Middle East.pdf

G8	trendmicro.com-Invitation to a Secret Event Uncovering Earth Yakos Campaigns.pdf
G9	trendmicro-earthkitsune.pdf
G10	trendmicro-x32dbg.pdf
G11	research.checkpoint.com-Pandas with a Soul Chinese Espionage Attacks Against Southeast Asian Government Entities.pdf
G12	mandiant.com-Stealing the LIGHTSHOW Part One North Koreas UNC2970.pdf
G13	blog.talosintelligence.com-YoroTrooper.pdf
G14	zscaler.com-apt37.pdf
G15	cta-2023-0330.pdf
G16	volexity.com-3CX Supply Chain Compromise Leads to ICONIC Incident.pdf
G17	mp-weixin-qq-com.translate.goog-scarcruft.pdf
G18	securelist.com-Following the Lazarus group by tracking DeathNote campaign.pdf
G19	uptycs.com-Cyber Espionage in India Decoding APT-36s New Linux Malware Campaign.pdf
G20	group-ib.com-SimpleHarm Tracking MuddyWaters infrastructure.pdf
G21	cta-2023-0420.pdf
G22	jamf.com-BlueNoroff APT group targets macOS with RustBucket Malware.pdf
G23	securelist.com-Tomiris called they want their Turla malware back.pdf
G24	research.checkpoint.com-Educated Manticore Iran Aligned Threat Actor Targeting Israel via Improved Arsenal of Tools.pdf
G25	research.checkpoint.com-Chain Reaction ROKRATs Missing Link.pdf
G26	news.sophos.com-A doubled Dragon Breath adds new air to DLL sideloading attacks.pdf
G27	malwarebytes.com-Uncovering RedStinger - Undetected APT cyber operations in Eastern Europe since 2020.pdf
G28	symantec-enterprise-blogs.security.com-Lancefly Group Uses Custom Backdoor to Target Orgs in Government Aviation Other Sectors.pdf
G29	group-ib.com-The distinctive rattle of APT SideWinder.pdf
G30	securelist.com-CloudWizard APT the bad magic story goes on.pdf

Grading Scheme:

- Completeness of extracted TTPs: (+50 marks)
- Comprehensive and to the point contextual information (+25 marks)
- Completeness of defensive recommendations (+25 marks)
- For each wrongly mapped TTP: (-5 marks)

- For each missed TTP: (-5 marks)
- For each wrong/missed contextual information: (-5 marks)
- For each non-related defensive recommendation: (-10 marks)