Asia-Pacific ATT&CK Community Workshop

Accelerating Identification of ATT&CK Techniques in Threat Intelligence Report

March 7th, 2025

Dr. Sareena Karapoola, NEC Corporation India
Takahiro Kakumaru, NEC Corporation

Agenda

1. Who we are
2. Cyber Intelligence Activities at NEC Corporation / Group
3. 4.5 Years Trends in the TOP 10 MITRE ATT&CK Techniques
4. Improving the Threat Report ATT&CK Mapping Efficiency
5. Results So Far & Way Forward
6. Acknowledgement

Who we are

NEC Corporation / Director of Cyber Intelligence

Takahiro Kakumaru, CISSP

- Over 20 years experience in R&D and security area
- Leading Cyber Intelligence Team

kakumaru@nec.com

NEC Corporation India / Senior Technical Manager

Dr. Sareena Karapoola

- Ph.D. in cyber security from the Indian Institute of Technology Madras, 2022.
- 20+ years experience in cybersecurity and R&D.

sareena.karapoola1@india..nec.com

Cyber Intelligence Activities at NEC Corporation / Group

Cyber Intelligence Activities at NEC Corporation / Group

NEC and NEC India are working together to regularly analyze emerging threat reports to glean cyber threat intelligence, including Indicators of Compromise (IOCs) and attack patterns (TTPs).

NEC Corporation

Cyber Intelligence Team

- CISO support
- PSIRT / IR support

Cyber Intelligence Activities

- Collecting
- Analyzing
- Reporting

Cooperation

Reports Functional and Operational Support

NEC Corporation India

Security Team

Cyber Security Segment
Digital Platform Delivery Unit

Cyber Intelligence Functions

- **MITRE ATT&CK** Analysis
- Customise **TRAM**
- Malware Analysis
- NEC Group's Global Community

ATT&CK Submissions / Contributions

- Identify novel techniques
- Propose our findings to MITRE ATT&CK Framework
- **53 published (ver.9-16)**

Threat Intelligence Sharing

- Sharing with global digital ecosystem (318K+ IoCs, 200K+ Attack Patterns)
- NEC Group

NEC Group's Global Community

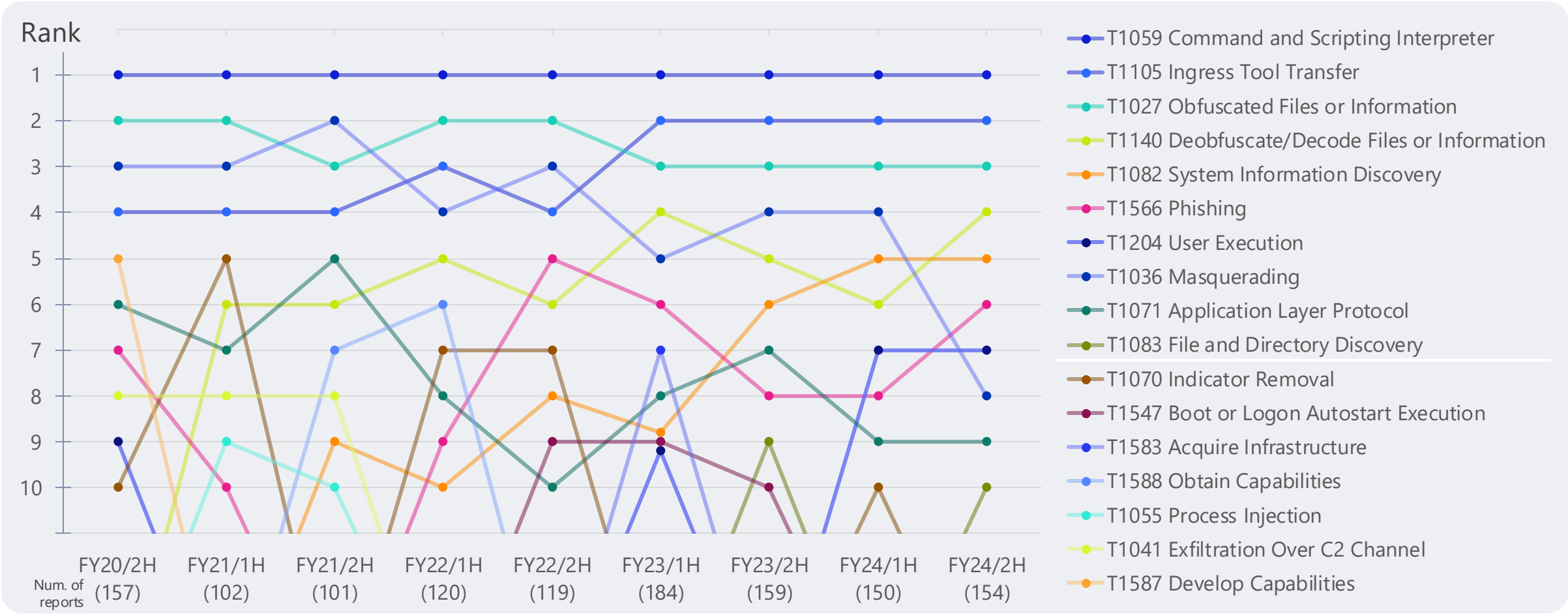
- Community building with NEC Country Affiliates worldwide

4.5 Years Trends in the TOP 10 **MITRE ATT&CK** Techniques

Results of analysis and data collection over 4.5 years.

4.5 Years Trends in the TOP 10 MITRE ATT&CK Techniques

Total number of reports analyzed over 4.5 years : 1,246 reports
Average number of reports analyzed per Half-Year : 138 reports



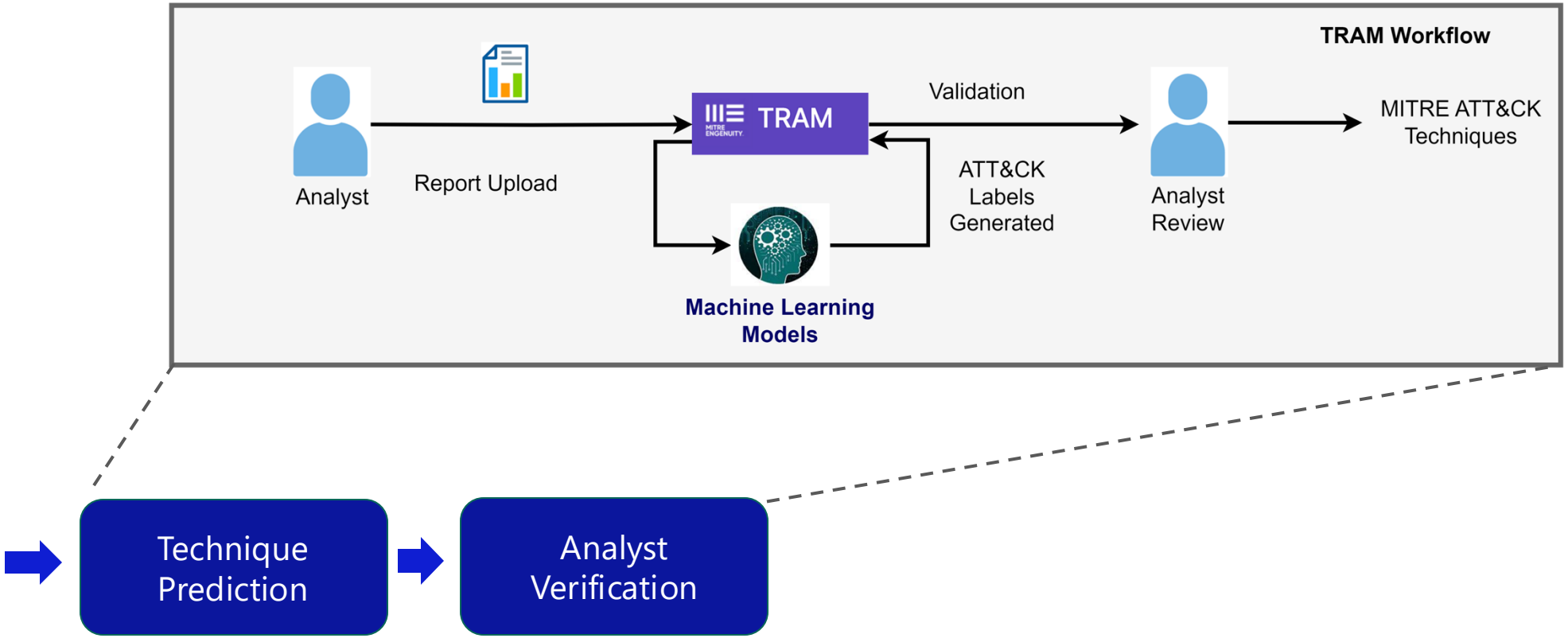
References / NEC Security Blog

- 2021.04.02 MITRE ATT&CK® Top 10 Most Common Tactics (2nd Half of 2020) | NEC Security Blog
  - https://jpn.nec.com/cybersecurity/blog/210402/index.html
- 2021.10.15 MITRE ATT&CK® Top 10 Most Common Tactics Vol.2 (1st Half of 2021) | NEC Security Blog
  - https://jpn.nec.com/cybersecurity/blog/211015/index.html
- 2022.05.27 MITRE ATT&CK® Top 10 Most Common Tactics Vol.3 (2nd Half of 2021) | NEC Security Blog
  - https://jpn.nec.com/cybersecurity/blog/220527/index.html
- 2022.11.11 MITRE ATT&CK® Top 10 Most Common Tactics (1st Half of 2022) | NEC Security Blog
  - https://jpn.nec.com/cybersecurity/blog/221111/index.html
- 2023.07.14 MITRE ATT&CK® Top 10 Most Common Tactics Vol.5 (2nd Half of 2022) | NEC Security Blog
  - https://jpn.nec.com/cybersecurity/blog/230714/index.html
- 2024.10.18 MITRE ATT&CK® Top 10 Most Common Tactics Vo.6 | NEC Security Blog
  - https://jpn.nec.com/cybersecurity/blog/241018/index.html

Improving the Threat Report **ATT&CK Mapping** Efficiency

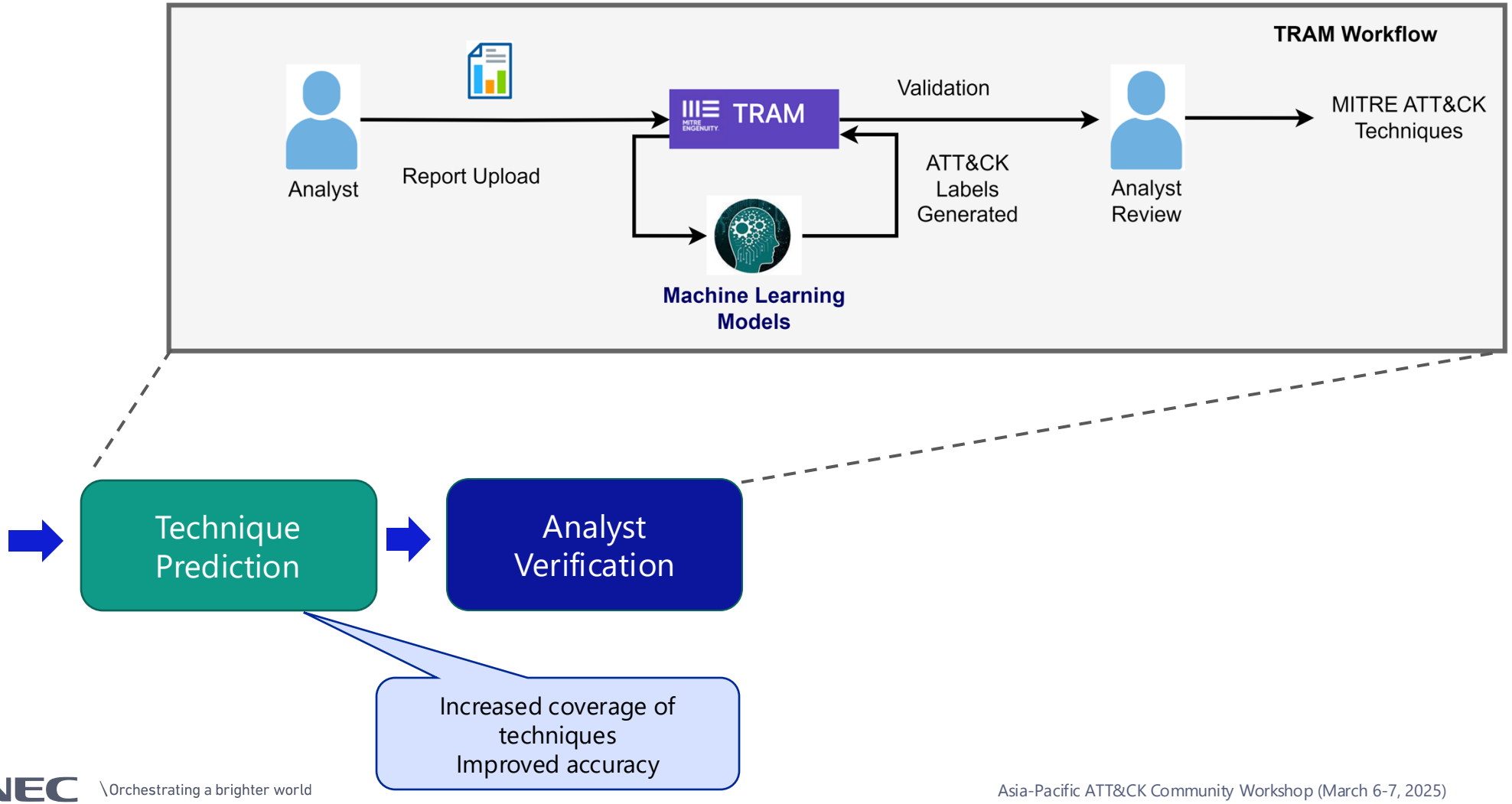
NEC Customized TRAM to accelerate MITRE ATT&CK Analysis

NEC have been using TRAM for cyber threat intelligence activities since 2020 and have continually customized it.



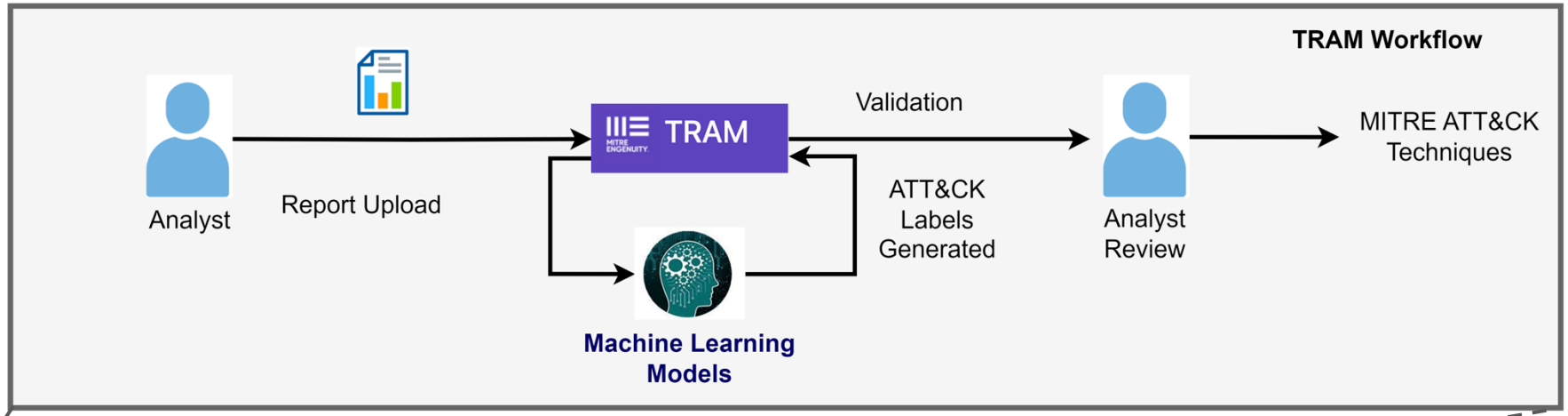
NEC Customized TRAM to accelerate MITRE ATT&CK Analysis

NEC have been using TRAM for cyber threat intelligence activities since 2020 and have continually customized it.



NEC Customized TRAM to accelerate MITRE ATT&CK Analysis

NEC have been using TRAM for cyber threat intelligence activities since 2020 and have continually customized it.



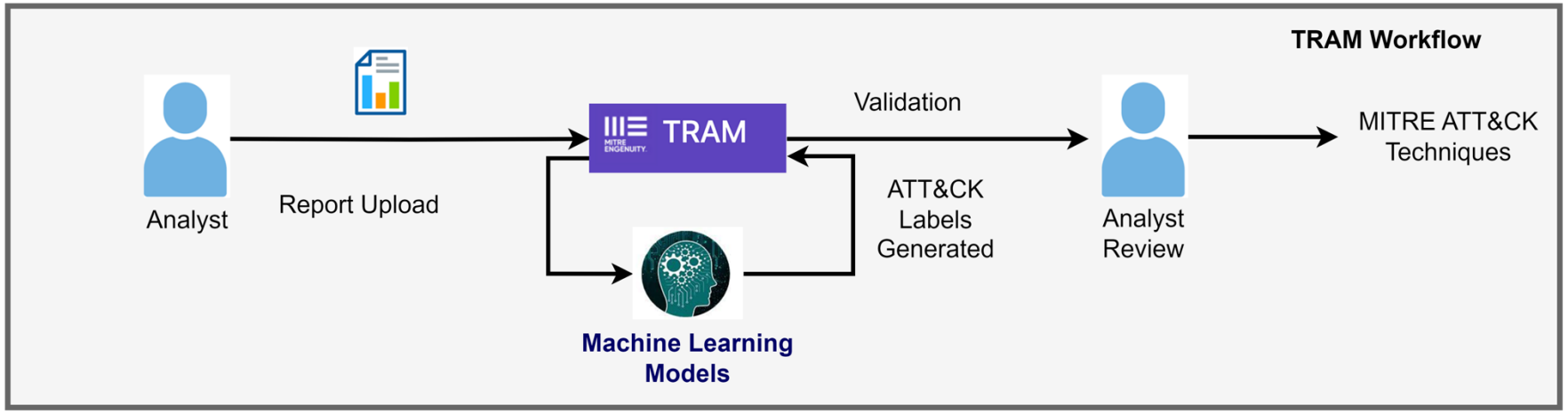
Technique Prediction → Analyst Verification → MITRE Recommendation → IoC Analysis → Standardization for Sharing

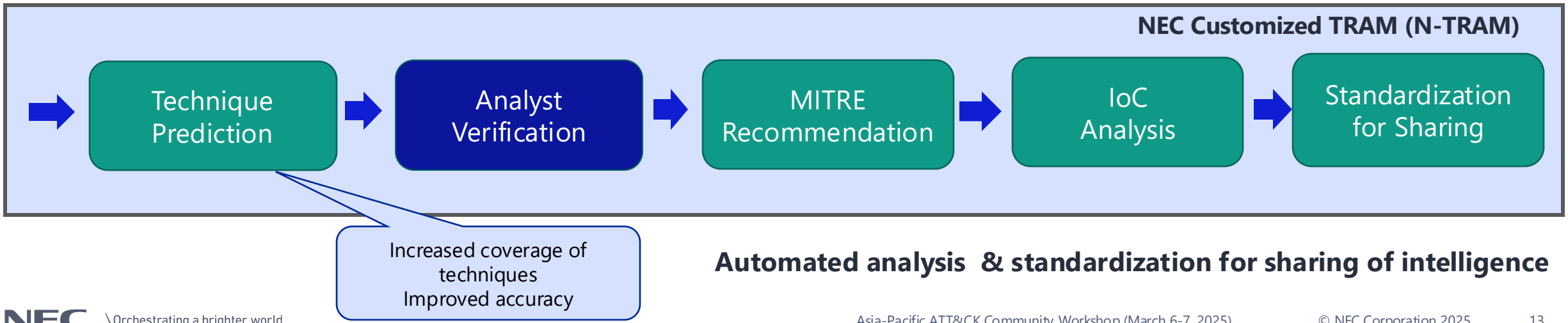
Increased coverage of techniques
Improved accuracy

Automated analysis & standardization for sharing of intelligence

NEC Customized TRAM to accelerate MITRE ATT&CK Analysis

NEC have been using TRAM for cyber threat intelligence activities since 2020 and have continually customized it.





Automated analysis & standardization for sharing of intelligence

Mapping Efficiency – Challenges & Way Forward

Challenges

Coverage

- Open TRAM support only **50 Techniques (81% F1-Score)**
- ATT&CK **(537 Techniques)**

Skewed representation

- >300 techniques have have less than 10 representation for effective learning

Algorithms

- Models performing low on Skewed data
- **Errors and Low Accuracy (22%)**

Data Enrichment

- How to ensure precise data with higher representation of each technique?
- Alternate data sources apart from data from MITRE ATT&CK
- Can the data sources be combined to ensure each technique have sufficient representation

Algorithms

How to enhance algorithms to perform on skewed data Explore Scibert and GPT?

Data Sources

What is the optimal data source for training the models?

ATT&CK 2024

- ATT&CK **(537 Techniques)**
- **Skewed**
- **Precise sentences from MITRE**

Historical data

- Database of sentences from threat reports analysed using NEC customized TRAM (N-TRAM)
- Verbose
- **May not be precise**

N-TRAM Analyst Comment

- Analyst reviewed interpretation of the mapping of sentence to ATT&CK ID
- **Precise**

Analysis of combinations of data sources and models

Datasets with Number of Techniques and frequency	Number of Techniques	SciBERT	GPT2
ATT&CK 2024	50	81.82%	78%
ATT&CK 2024 + Historical Data	50	78.36%	74%
ATT&CK 2024 + Historical Data+ Analyst comments	50	81.88%	81.21%
ATT&CK 2024 + Analyst comment	50	84.58%	83.48%
ATT&CK 2024 + Historical Data	236	32.32%	78.36%
ATT&CK 2024+ Analyst >20	236	47.25%	61.74%

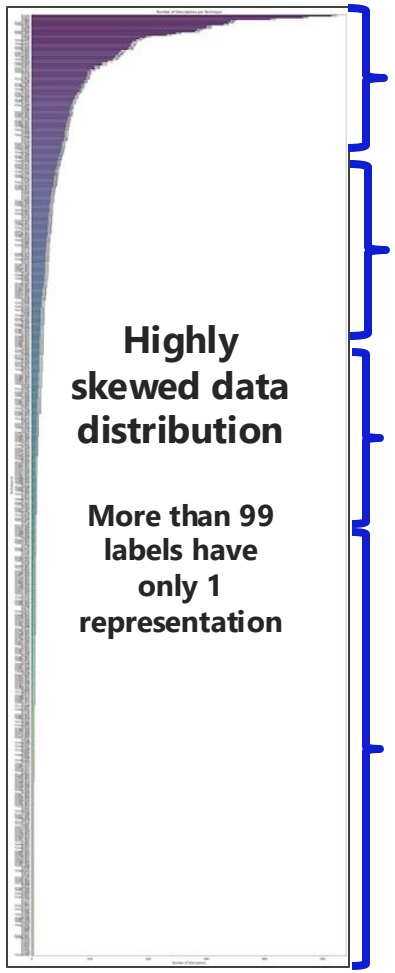
Utilizing the Historical data + Analyst comments can improve performance

On data with larger number of techniques, GPT2 is performing better

Optimizations needed to handle skewed data

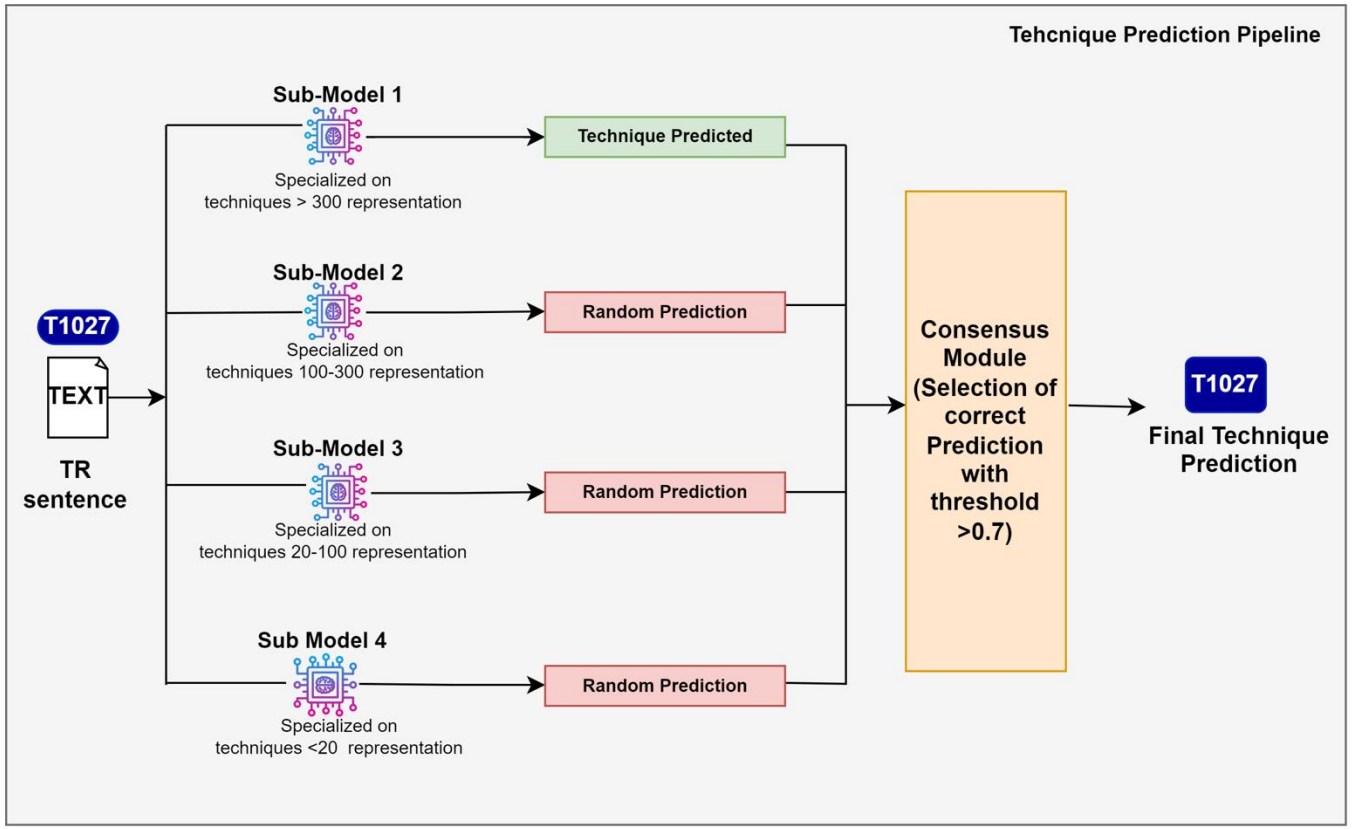
Ensemble of Predictors

Handling skewed data with specialized predictors trained for subset of data



Divide the technique space among specialized models

Data Augmentation



Results So Far & Way Forward

	Precision	Recall	F1-Score
GPT2 trained on **283 Techniques**	0.80	0.95	**0.86**

1. **Utilizing historical data along with analyst reviewed comments increases performance**
2. **Divide & Conquer strategy to address skewed data is beneficial**
3. **Key is to have optimal division of the technique space among the models**
4. **Future Optimizations:**
   - Distribution of technique space based on grouping of tactics

Thanks to

NEC Corporation

Ai Kimura
Akiko To
Daisuke Maeda
Hiroki Nagahama
Jun Hirata
Michibi Uehama
Riku Katsuse
Satoshi Gunji
Shun Miyazaki
Takemasa Kamatani
Toshiki Takeuchi
Wataru Takahashi
Yasuhito Kawanishi
Yoshihiro Kori
Yuto Takahashi

NEC Corporation India

Pooja Natarajan
Dhanvarshini Gopalasamy
Abhishek Dhiman
Vijay Chandran
Manikantan Srinivasan

\Orchestrating a brighter world