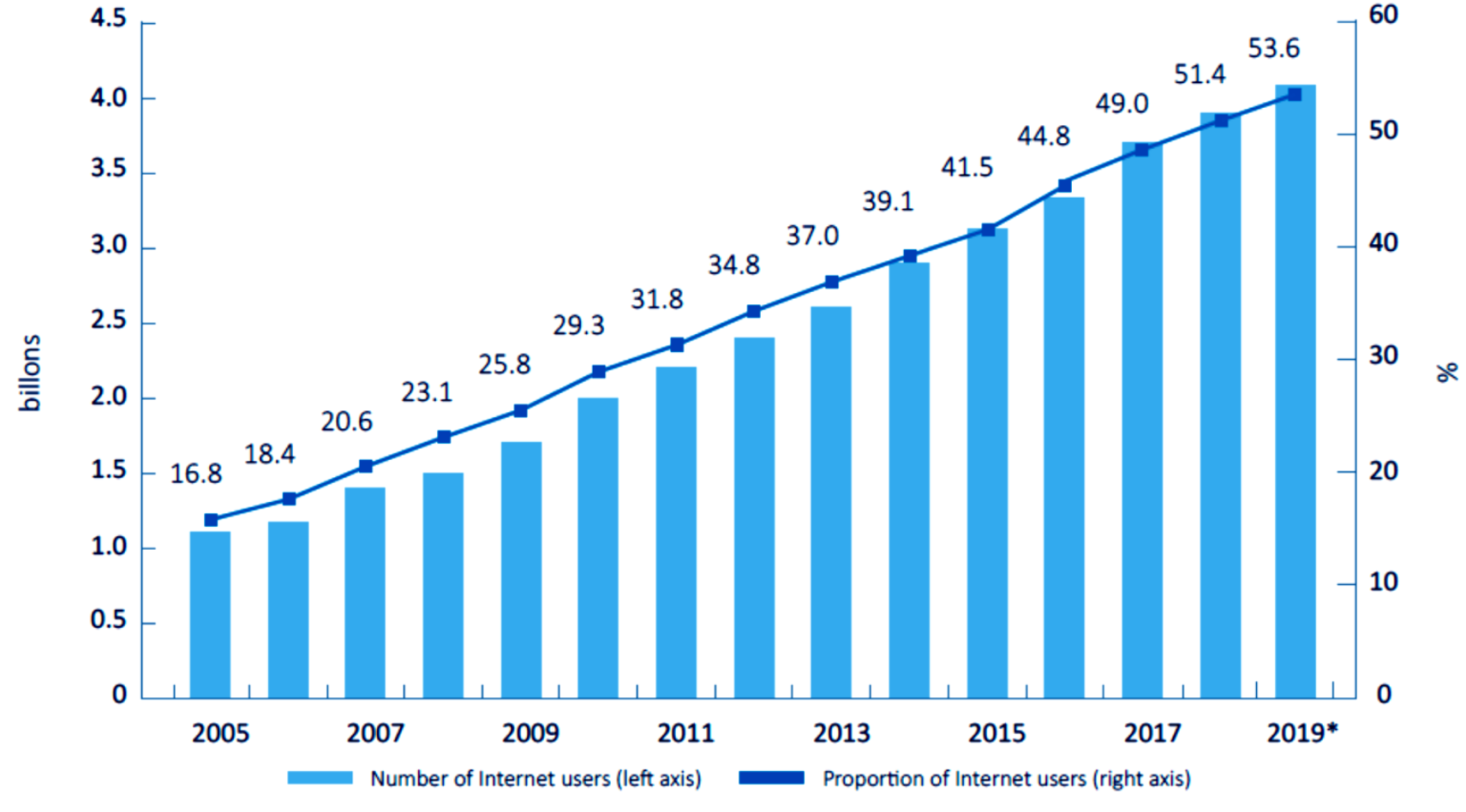
NTRA
National Telecom Regulatory Authority
الجـــهاز القـــومي لتنـــظيم الإتصـالات

EGYPT
National Telecom Regulatory Authority

Malware Analysis and Reverse Engineering Department

Internet Users



Source: ITU Facts and Figures 2019 report.

Applications

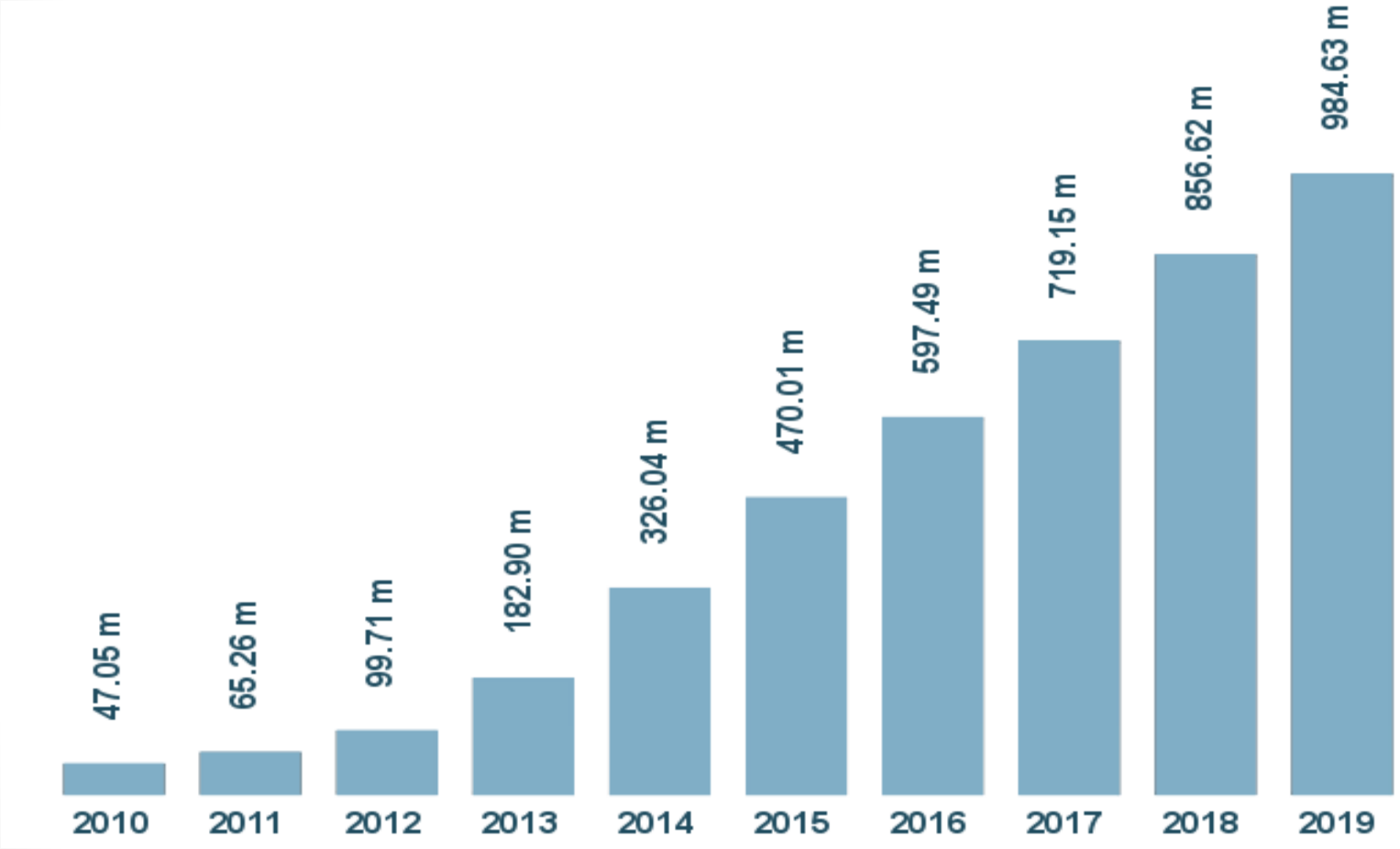
There were 23 million software developers in 2018, this number is expected to reach 26,4 million by the end of 2019 and 27,7 million by 2023 (**Evans Data Corporation**)

2.7 billion smartphone users and 1.35 billion tablet users across the world (**Statista**)

There were 178 billion app downloads in 2017, 205 billion downloads in 2018, and an estimated 258 billion downloads in 2022. (**Statista**)

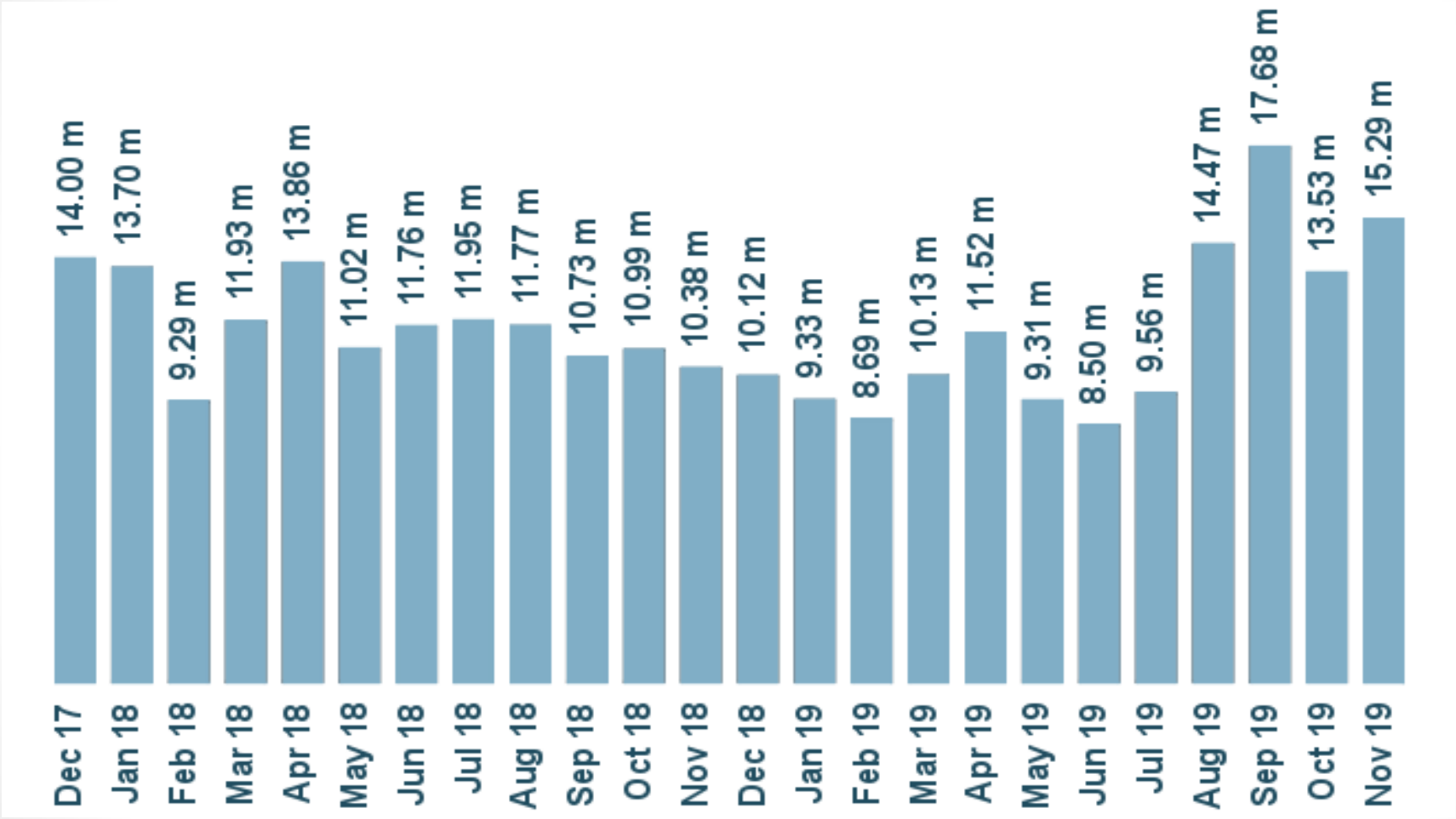
Around 90% of smartphone time is spent on apps. (**eMarketer**)

Malicious software



Source: AV-TEST - independent research institute for IT security

New malicious software



Source: AV-TEST - independent research institute for IT security

Impact

It is predicted cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015 (Cybersecurity Ventures)

Data breaches exposed 4.1 billion records in the first half of 2019. (RiskBased)

Hackers attack every 39 seconds, on average 2,244 times a day. (University of Maryland)

While overall ransomware infections were down 52%, enterprise infections were up by 12% in 2018. (Symantec)

62% of businesses experienced phishing and social engineering attacks in 2018. (Cybint Solutions)

Impact

The global cybersecurity market is expected to develop from $120 billion in 2017 to $300 billion by 2024. (Global Market Insights)

Cybersecurity products and services will exceed $1 trillion in total value from 2017 to 2021. (Cybersecurity Ventures)

The global cybercrime economy earns around $1.5 trillion yearly. (SSLStore)

The top 4 countries as per venture capital dollars invested in cybersecurity are the US, Israel, UK, and Canada. (BusinessFacilities)

Singapore launched the very first commercial cyber risk pool in the world. It will commit up to $1 billion in risk capacity. (Yahoo)

Vision

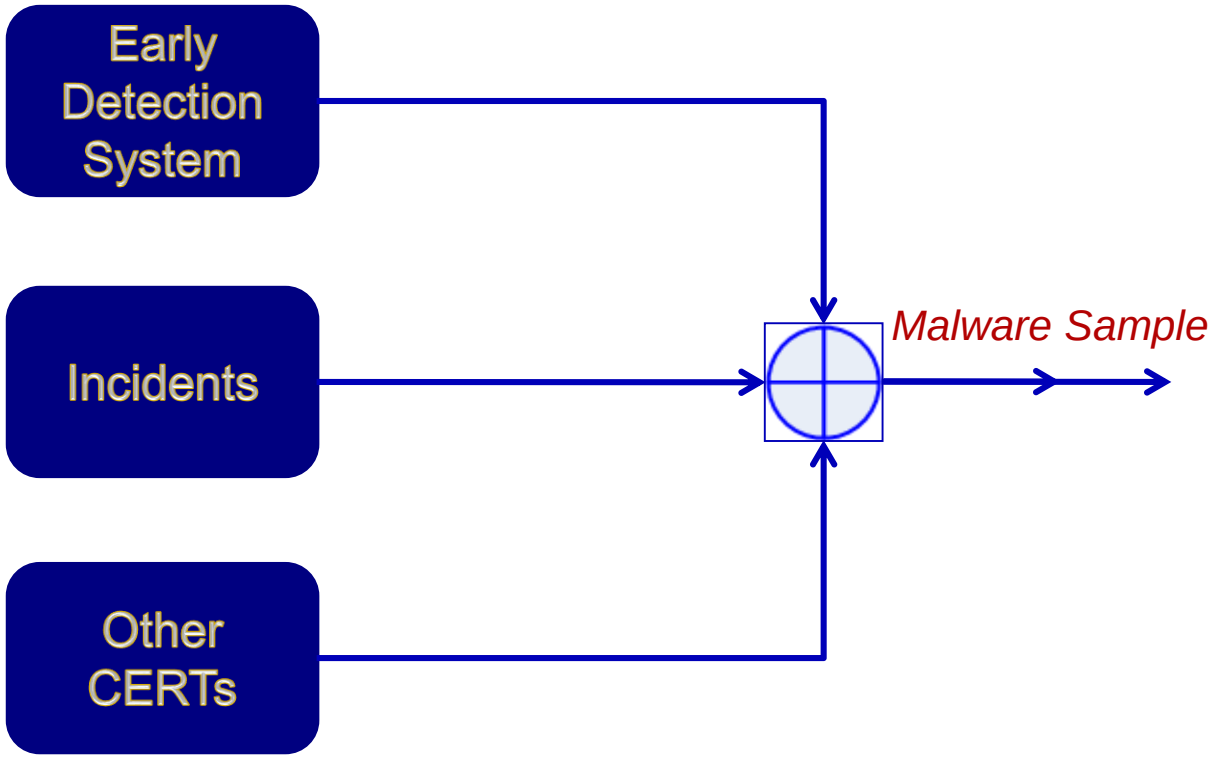
Possess the knowledge and proficiency to automatically detect malicious activities target Egyptian information infrastructure in proactive manner that making Egypt Secure and resilient to cyber threats.

Mission

- The malware analysis process is used to identify and analyze the new malware samples. Then, provide mitigation techniques
- Conduct research based on artificial intelligence/machine learning techniques to automatically detect new malware samples.

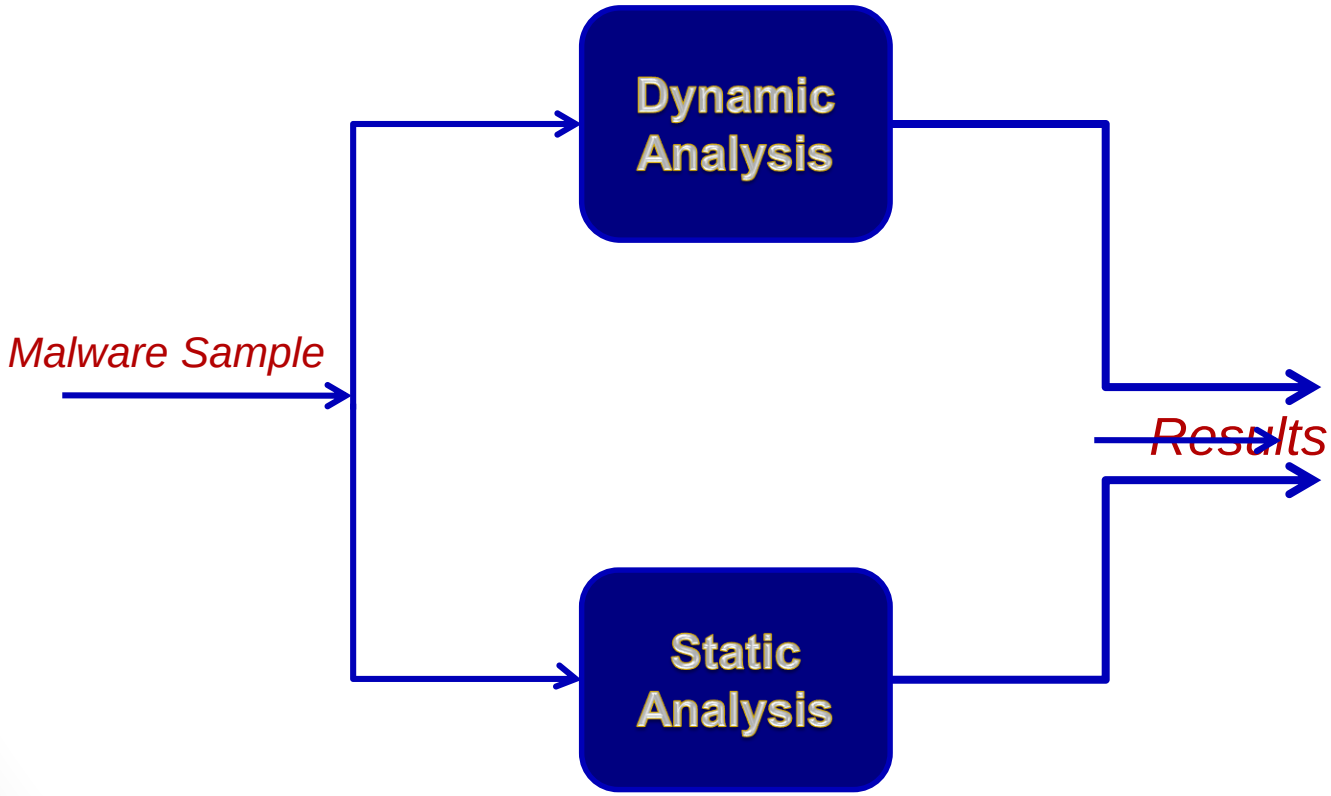
Work-Flow

- ***Step 1: Sample Collection***



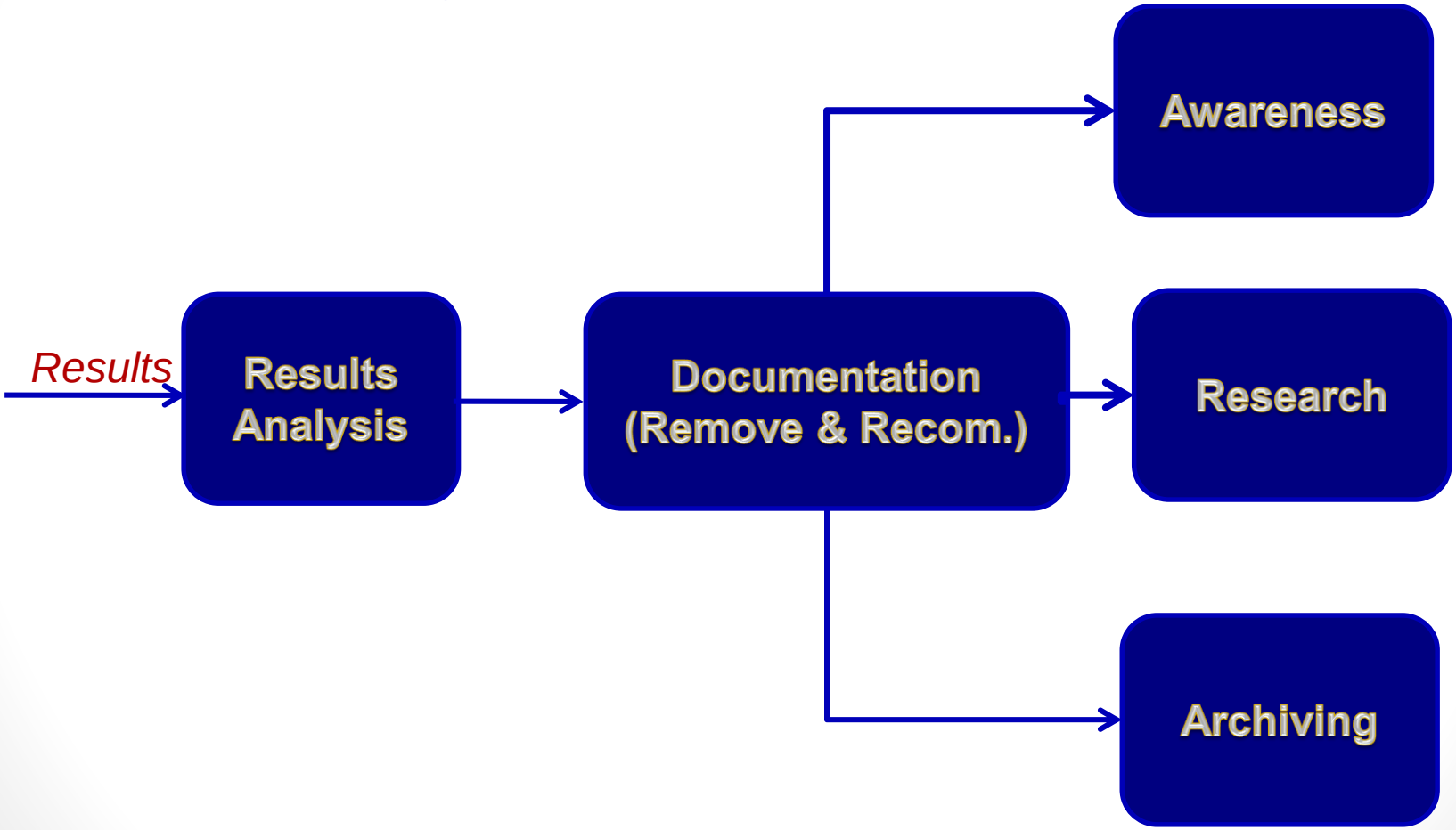
Work-Flow

- ***Step 2: Sample Analysis***



Work-Flow

- ***Step 3: Reporting***



Egyptian Anti-Malware

- It is under developing by EG-CERT team
- It is based on AI/ML techniques.
- First version was released June, 2018.
- Second version was released June, 2019

Cyber Attacks Early Detection System

The main objective of the project is to monitor malware activities in various sectors and to provide cybersecurity teams better visibility for early detection of new malware.

This project will help increase the efficiency of the Egyptian anti-malware project through information obtained from this project.

In turn, this project will help reduce the spread of malware targeting the information infrastructure of the Egyptian cyberspace.

Publications

1. S. Sayed, Rania R. Darwish, Sameh A. Salem, "A Real-Time Approach for Detecting Malicious Executables," Proceedings of the International Conference on Systems Science 2013 (ICSS 2013), Volume 240, 2014, pp 355-364
2. Ahmed A. Awad, Samir G. Sayed, Sameh A. Salem, "A network-based framework for RAT-bots detection," Proceedings of the 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON).
3. Ahmed A. Awad, Samir G. Sayed, Sameh A. Salem, "A Host-based framework for RAT-bots detection," Proceedings of the IEEE International Conference on Computer and Applications (ICCA).
4. Doaa Wael, Ahmed Shosha, Samir G. Sayed, "Malicious VBScript detection algorithm based on data-mining techniques," In Proceedings of the International Conference on Advanced Control Circuits Systems (ACCS) Systems & International Conference on New Paradigms in Electronics & Information Technology (PEIT), 2017
5. Samir G. Sayed , Mohamed Shawkey, "Data Mining Based Strategy for Detecting Malicious PDF Files," In Proceedings of the 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications (IEEE TrustCom-18), 2018.
6. May Medhat; Samir G. Sayed; Nashwa Abdelbaki, "A New Static-based Framework for Ransomware Detection," In Proceedings of the 16th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2018), 2018.
7. Doaa Wael; Samir G. Sayed; Nashwa Abdelbaki, "Enhanced Approach to Detect Malicious VBScript files Based on Data Mining Techniques", In Proceedings of Fifth International Workshop on Privacy and Security in HealthCare 2018.
8. Ahmed A. Awad, Samir G. Sayed, Sameh A. Salem, "Collaborative Framework for Early Detection of RAT-Bots Attacks," IEEE Access, Vol.7, pp 71780-717890, 2019.