SOLARMARKER'S SECRETS
THROUGH EXPERT THREAT HUNTING
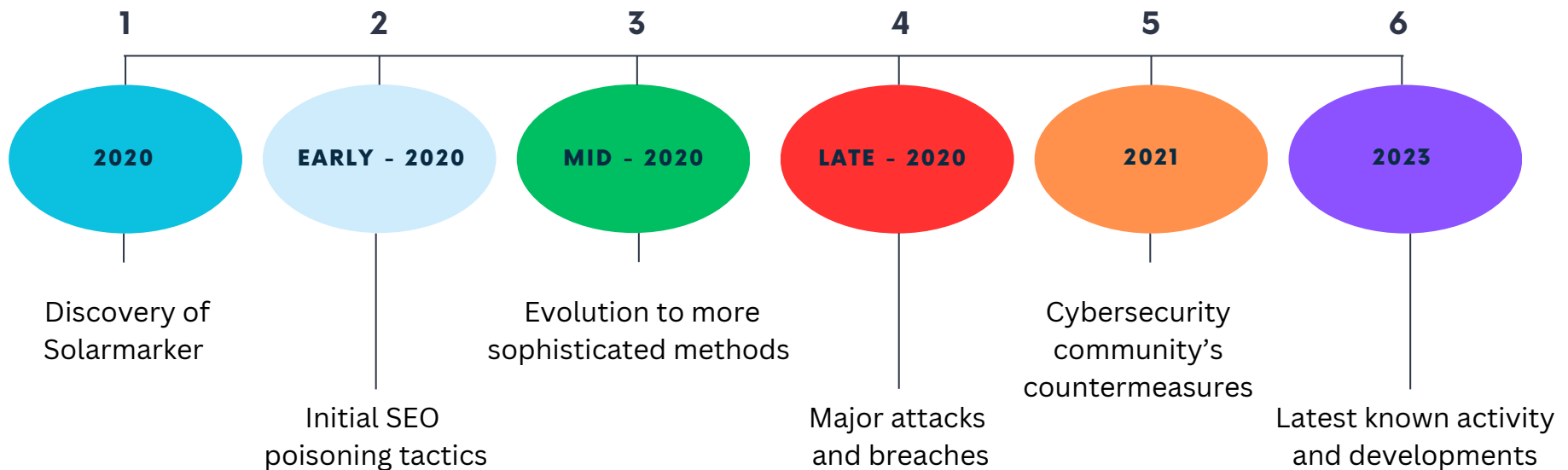
THREAT HUNTING OVERVIEW

Proactive Cyber Defense: Threat hunting is the vigilant search for hidden adversaries. It's an essential, continuous process that goes beyond traditional security to safeguard digital realms.
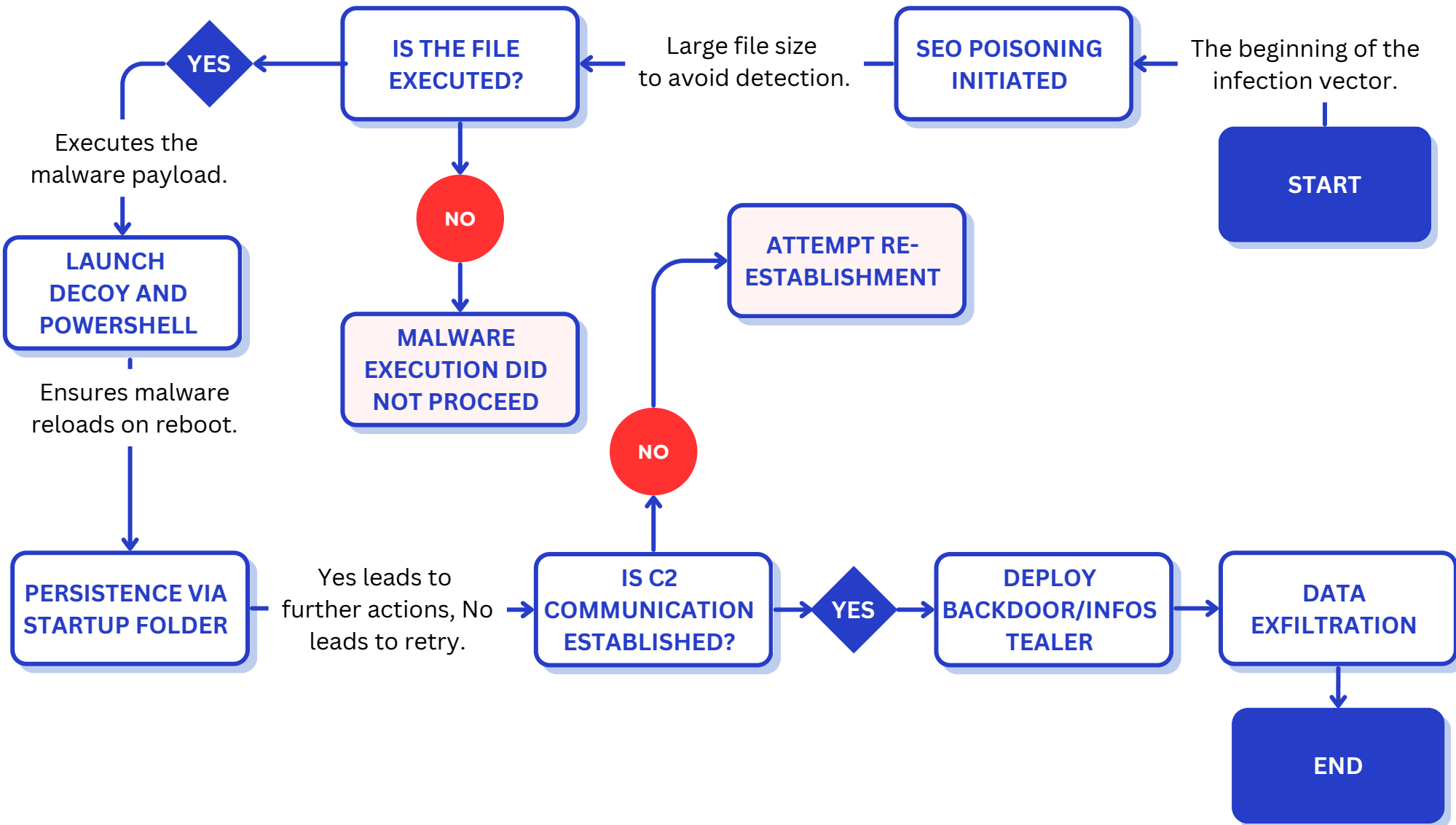
Tracking digital traces to uncover hidden threats.

Collaborative efforts to fortify defenses against cyber adversaries.

Utilizing advanced tools for deep network analysis.

Deciphering data patterns to predict and prevent attacks.

THE SOLARMARKER CAMPAIGN

1	2	3	4	5	6
2020	**EARLY - 2020**	**MID - 2020**	**LATE - 2020**	**2021**	**2023**

Discovery of Solarmarker

Initial SEO poisoning tactics

Evolution to more sophisticated methods

Major attacks and breaches

Cybersecurity community's countermeasures

Latest known activity and developments

SOLARMARKER TACTICS, TECHNIQUES, AND PROCEDURES (TTPS)

START → The beginning of the infection vector. → **SEO POISONING INITIATED** → Large file size to avoid detection. → **IS THE FILE EXECUTED?**

IS THE FILE EXECUTED?
- **YES** → Executes the malware payload. → **LAUNCH DECOY AND POWERSHELL** → Ensures malware reloads on reboot. → **PERSISTENCE VIA STARTUP FOLDER**
- **NO** → **MALWARE EXECUTION DID NOT PROCEED**

PERSISTENCE VIA STARTUP FOLDER → Yes leads to further actions, No leads to retry. → **IS C2 COMMUNICATION ESTABLISHED?**

IS C2 COMMUNICATION ESTABLISHED?
- **NO** → **ATTEMPT RE-ESTABLISHMENT**
- **YES** → **DEPLOY BACKDOOR/INFOSTEALER** → **DATA EXFILTRATION** → **END**

METHODICAL VIGILANCE

Pinpoint potential cyber threat scenarios.

Develop theories from threat intelligence.

Collect data to investigate threats.

Analyze data for unusual activities.

Probe anomalies for hidden threats.

Document findings and actions taken.

Improve methods with continuous feedback.

FUTURE OF THREAT HUNTING

Integration of AI and ML

Emphasizing the role of artificial intelligence and machine learning in automating threat detection and response.

Advanced Analytics

The use of sophisticated analytics to process large datasets and identify subtle patterns of malicious activity.

Proactive Threat Identification

Moving from reactive to proactive measures in identifying and mitigating threats before they cause harm.

Collaborative Threat Intelligence

Sharing insights and data across organizations to build a collective defense against emerging threats.

Adaptive Security Architectures

Developing flexible and adaptive security frameworks that can evolve with the changing threat landscape.

Continuous Learning and Adaptation

Emphasizing the importance of ongoing education and training for cybersecurity teams.

01 02 03 04 05 06