Rule Framework: A Core Tool for Threat-Centric Security Strategy

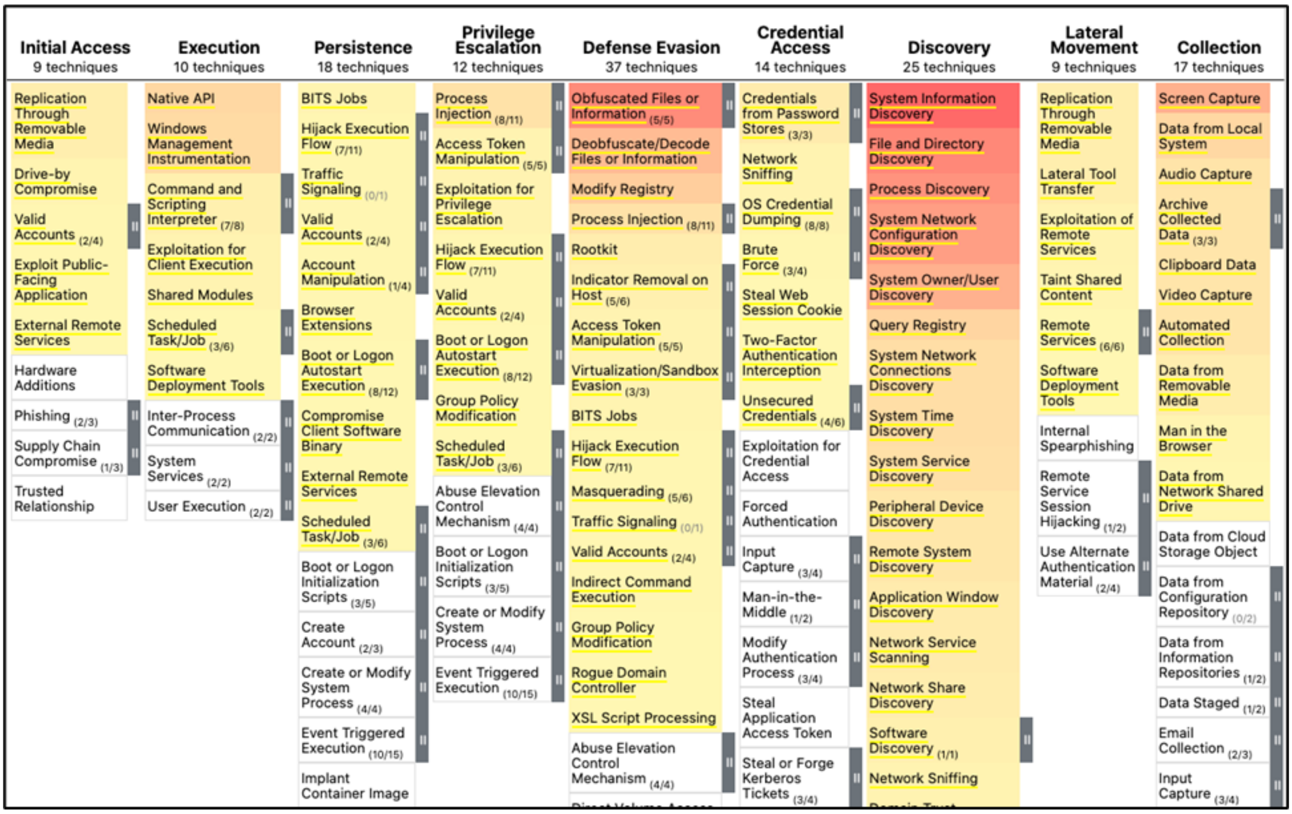
Ki-tack Seo / Security Operations & CERT Team, Team Leader

■ The Era of Advanced Persistent Threats

Cybersecurity is no longer just an IT issue; it has become a strategic priority directly tied to organizational survival. evolving into a strategic imperative intrinsically linked to the survival of organizations. Particularly, sophisticated attacks such as Advanced Persistent Threats (APTs), supply chain attacks, and ransomware are posing significant threats to major corporations and public institutions worldwide. Consequently, there has been a strategic shift in information security paradigms from traditional prevention-focused models to those centered on threat detection and response. At the core of this transformation lies the enhancement of detection rule-sets and methodologies, with the MITRE ATT&CK framework standing out as a quintessential security strategy model. The ATT&CK framework serves as a comprehensive knowledge base constructed on the actual behaviors of adversaries, thereby helping organizations design effective threat-focused security strategies.

■ What is the MITRE ATT&CK Framework?

MITRE ATT&CK, an acronym for Adversarial Tactics, Techniques, and Common Knowledge, is a systematically organized knowledge base matrix that categorizes the tactics, techniques, and procedures (TTPs) employed by adversaries in real-world scenarios.



Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Replication Through Removable Media	Native API	BITS Jobs	Process Injection (8/11)	Obfuscated Files or Information (5/5)	Credentials from Password Stores (3/3)	System Information Discovery	Replication Through Removable Media	Screen Capture
Drive-by Compromise	Windows Management Instrumentation	Hijack Execution Flow (7/11)	Access Token Manipulation (5/5)	Deobfuscate/Decode Files or Information	Network Sniffing	File and Directory Discovery	Lateral Tool Transfer	Data from Local System
Valid Accounts (2/4)	Command and Scripting Interpreter (7/8)	Traffic Signaling (0/1)	Exploitation for Privilege Escalation	Modify Registry	OS Credential Dumping (8/8)	Process Discovery	Exploitation of Remote Services	Audio Capture
Exploit Public-Facing Application	Exploitation for Client Execution	Valid Accounts (2/4)	Hijack Execution Flow (7/11)	Process Injection (8/11)	Brute Force (3/4)	System Network Configuration Discovery	Taint Shared Content	Archive Collected Data (3/3)
External Remote Services	Shared Modules	Account Manipulation (1/4)	Valid Accounts (2/4)	Rootkit	Steal Web Session Cookie	System Owner/User Discovery	Remote Services (6/6)	Clipboard Data
Hardware Additions	Scheduled Task/Job (3/6)	Browser Extensions	Boot or Logon Autostart Execution (8/12)	Indicator Removal on Host (5/6)	Two-Factor Authentication Interception	Query Registry	Software Deployment Tools	Video Capture
Phishing (2/3)	Software Deployment Tools	Boot or Logon Autostart Execution (8/12)	Group Policy Modification	Access Token Manipulation (5/5)	Unsecured Credentials (4/6)	System Network Connections Discovery	Internal Spearphishing	Automated Collection
Supply Chain Compromise (1/3)	Inter-Process Communication (2/2)	Compromise Client Software Binary	Scheduled Task/Job (3/6)	Virtualization/Sandbox Evasion (3/3)	Exploitation for Credential Access	System Time Discovery	Remote Service Session Hijacking (1/2)	Data from Removable Media
Trusted Relationship	System Services (2/2)	External Remote Services	Abuse Elevation Control Mechanism (4/4)	BITS Jobs	Forced Authentication	System Service Discovery	Use Alternate Authentication Material (2/4)	Man in the Browser
	User Execution (2/2)	Scheduled Task/Job (3/6)	Boot or Logon Initialization Scripts (3/5)	Hijack Execution Flow (7/11)	Input Capture (3/4)	Peripheral Device Discovery		Data from Network Shared Drive
		Boot or Logon Initialization Scripts (3/5)	Create or Modify System Process (4/4)	Masquerading (5/6)	Man-in-the-Middle (1/2)	Remote System Discovery		Data from Cloud Storage Object
		Create Account (2/3)	Event Triggered Execution (10/15)	Traffic Signaling (0/1)	Modify Authentication Process (3/4)	Application Window Discovery		Data from Configuration Repository (0/2)
		Create or Modify System Process (4/4)		Valid Accounts (2/4)	Steal Application Access Token	Network Service Scanning		Data from Information Repositories (1/2)
		Event Triggered Execution (10/15)		Indirect Command Execution	Steal or Forge Kerberos Tickets (3/4)	Network Share Discovery		Data Staged (1/2)
		Implant Container Image		Group Policy Modification		Software Discovery (1/1)		Email Collection (2/3)
				Rogue Domain Controller		Network Sniffing		Input Capture (3/4)
				XSL Script Processing				
				Abuse Elevation Control Mechanism (4/4)				

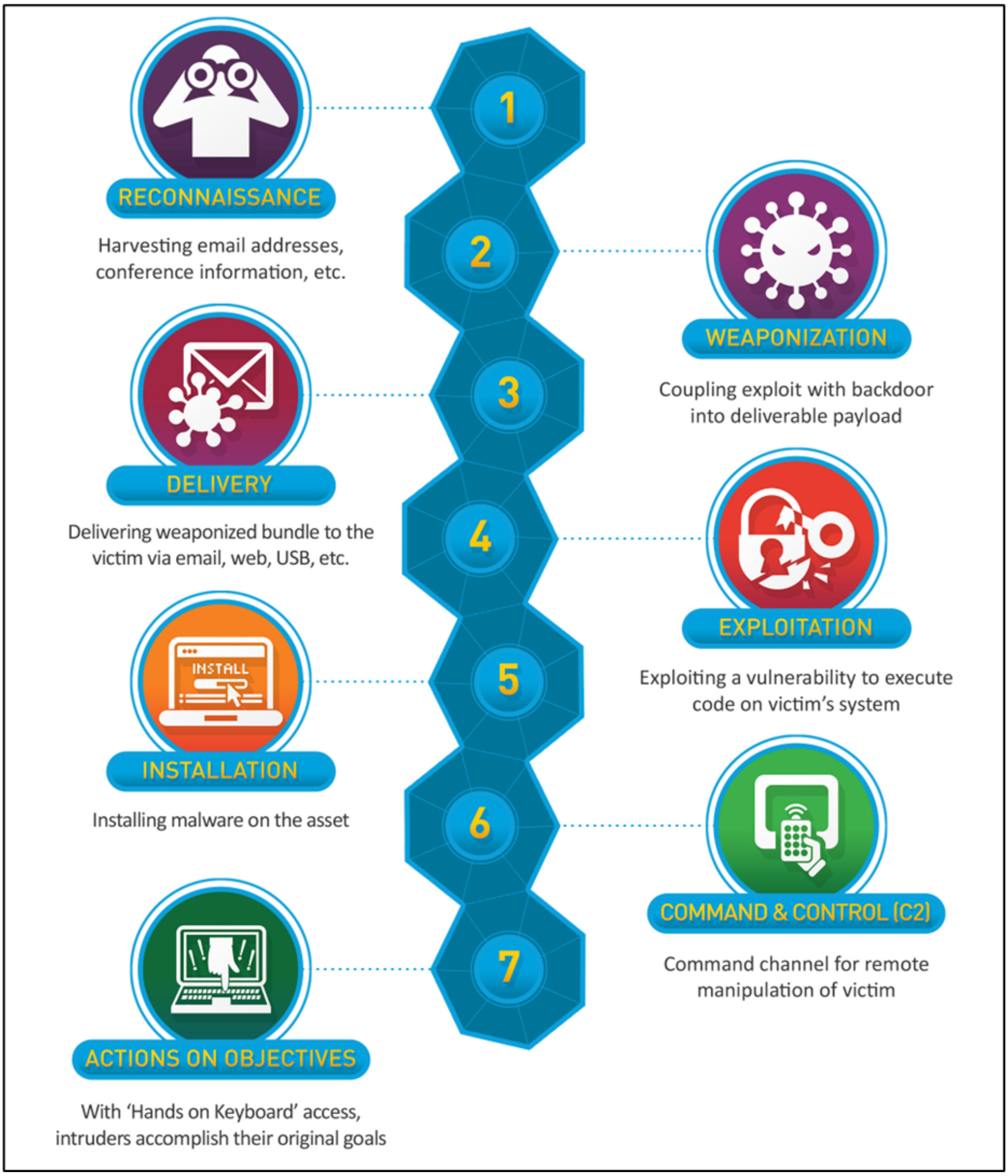
* Source: MITRE ATT&CK Official Website

Figure 1. Excerpt from the MITRE ATT&CK Matrix - Navigator

Attacks typically progress based on a series of sequential actions, with each phase distinguished by specific tactics and techniques. For instance, an attacker may initially attempt to gain initial access, followed by privilege escalation, internal reconnaissance, command and control (C2), and data exfiltration. The MITRE ATT&CK framework categorizes attacks according to these phases, offering detailed descriptions of techniques, detection indicators, and mitigation strategies. Currently, it provides three matrices: Enterprise, Mobile, and ICS, which can be applied to diverse environments such as corporate security, industrial control system security, and mobile security.

■ Composition of Tactics, Techniques, and Procedures (TTPs) in the MITRE ATT&CK Framework

The crux of the MITRE ATT&CK framework lies in its systematic modeling of adversarial behavior through distinct Tactics, which represent the stages of an attack, and the specific Techniques employed at each stage. This framework elucidates the objectives and methodologies utilized by attackers during the execution of a cyber assault, thereby enabling organizations to structurally analyze real-world threat scenarios.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

* Source: Lockheed Martin Official Website

Figure 2. The Cyber Kill Chain Model Released by Lockheed Martin

As illustrated in [Figure 2], cyber threat activities unfold in a sequential manner. Delving deeper into each phase, the initial stage involves the attacker attempting 'Initial Access' to the system. This is executed through methods such as phishing emails, malicious links, or exploiting vulnerabilities in user behavior or external interfaces, including known user credentials. The primary objective of this phase is to establish a foothold that facilitates entry into the internal network. Subsequently, the 'Execution' phase ensues, wherein the attacker, having gained access, endeavors to execute malicious code to secure control over the system. This encompasses activities such as script execution, command injection, and the exploitation of processes. This phase serves as the gateway through which the attacker effectuates malicious operations within the system.

The term 'Persistence' refers to the mechanisms established by an attacker to maintain a prolonged presence within a system. Techniques such as service registration or the installation of autorun programs are employed to ensure that the malicious code continues to operate even after a system reboot or user logout. The subsequent phase, known as 'Privilege Escalation,' involves elevating the privileges of a standard user to those of an administrator or root, thereby enabling broader access to the system. Following this, the 'Defense Evasion' stage employs techniques to bypass or neutralize security solutions and logging systems. This includes methods such as obfuscating malicious files or employing code injection to circumvent antivirus software. This stage is critical for avoiding detection and facilitating ongoing attacks. During the 'Credential Access' phase, the attacker seeks to collect user IDs or passwords within the system to move laterally to other systems or to gain additional privileges. This is achieved by extracting password hashes from memory or installing keyloggers. The 'Discovery' phase involves the reconnaissance of the internal network's structure, user directories, and system information. Attackers utilize this intelligence to plan subsequent attack phases or to establish pathways for lateral movement.

The phase at which malicious activities begin to proliferate extensively is referred to as the 'Lateral Movement' stage. This involves the attacker transitioning from one system to another, employing methods such as credential theft or remote command execution as primary means. Through this process, the attacker gradually gains access to critical systems. Once the objectives of the attack become more defined, the 'Collection' phase commences. During this stage, the attacker accumulates specific data, such as documents, customer information, certificates, and log files, which are stored for potential future exfiltration or manipulation. The process of transmitting the collected information to external entities constitutes the 'Command and Control (C2)' phase. Here, the attacker establishes a connection with an external C2 server via malicious software, facilitating the exchange of commands or the transmission of data. Typically, encrypted communications or transmissions masquerading as legitimate protocols are employed.

The final phase of an attack is termed 'Impact,' which encompasses the actual infliction of damage, such as the degradation of system availability, data corruption, and ransomware infection. At this juncture, the attacker endeavors to achieve objectives such as data deletion, system destruction, and monetary extortion.

In this manner, the Tactics, Techniques, and Procedures (TTPs) of the MITRE ATT&CK framework clearly describe each phase of an attack, thereby facilitating the tracking and analysis of adversaries' mindsets and behavioral patterns. This enables threat response organizations to develop stage-specific defensive strategies and to construct more sophisticated detection rules and response scenarios.

■ Analysis of APT Attack Cases

Through real-world attack scenarios, one can comprehend the application of strategies and techniques from the ATT&CK framework in practical settings.

- APT29 (Cozy Bear)

  In the SolarWinds supply chain attack, techniques such as DLL Side-Loading (T1574.002) and the injection of malicious code into legitimate processes (T1055) were employed.
- Lazarus Group

  In attacks targeting financial institutions, a tactical combination of techniques was employed, including phishing (T1566.001), credential dumping (T1003), and lateral movement via SMB (T1021.002).
- FIN7

  Malicious documents were distributed targeting POS systems (T1203), followed by data collection from local systems (T1005) and exfiltration of the gathered information to external servers (T1041).

In the aforementioned case, each attack flow is meticulously mapped to the MITRE ATT&CK techniques and tactics, thereby enabling the reconstruction of attacks or the formulation of detection policies. This approach transcends the mere enumeration of techniques employed by adversary groups, instead mapping their entire attack flow into a 'Tactics, Techniques, and Procedures (TTPs) framework.' This allows for the visualization of potential detection and response measures at each stage.

- Lazarus Group: Attacks targeting financial institutions and cryptocurrency exchanges.

Lazarus Group, a threat actor reportedly linked to North Korea, is an APT organization that has consistently targeted financial institutions and cryptocurrency exchanges. Their operations typically involve gaining initial access through phishing emails, social engineering tactics, and exploitation of web vulnerabilities. Following initial compromise, they proceed to obtain credential access and conduct lateral movement within the network to reach high-value asset systems.

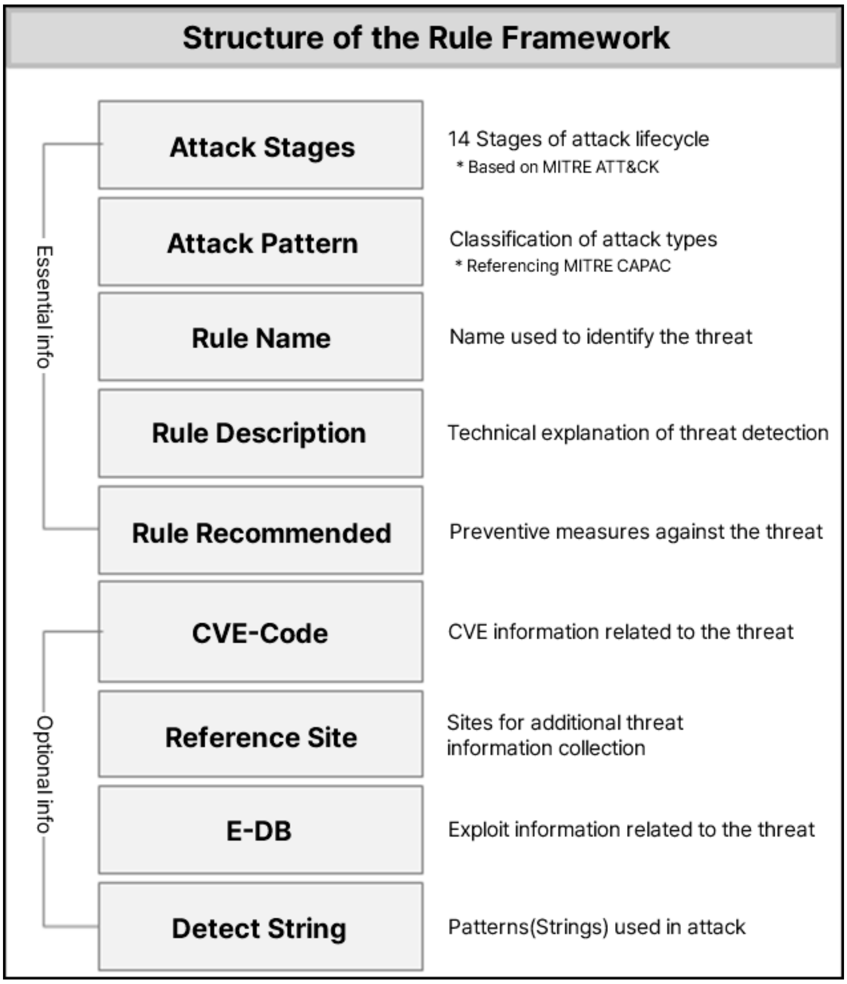
When analyzed through the MITRE ATT&CK framework, Lazarus's phishing campaigns align with the T1566.001 technique (Spear Phishing Attachment). Subsequent privilege escalation is categorized under T1068 (Exploitation for Privilege Escalation), while credential theft corresponds to T1003 (Credential Dumping). The group also accessed internal systems via RDP connections (T1021.001) and exfiltrated sensitive data to external C2 servers (T1041). In practical cybersecurity operations, such correlation analysis enables security teams to incorporate the tactics and techniques used by Lazarus into detection policies. Moreover, it serves as a foundational reference for conducting effective threat hunting.

Table 1. Example of Applying the MITRE ATT&CK Framework to Analyze Attack Cases

As exemplified in APT cases, the MITRE ATT&CK framework facilitates a comprehensive understanding of complex attack vectors by tactically structuring the flow of these incursions. This enables a clear identification of the attack's origin, the techniques employed, and the stages at which detection and defense were feasible. Furthermore, it serves as an effective tool for constructing preemptive detection rules based on historical attack instances or for developing threat hunting scenarios.

■ Secudium Center – Rule Framework

The Rule Framework transcends being merely a theoretical tool, playing a pivotal role in enabling real-world security organizations to systematically comprehend adversarial behaviors and enhance their response capabilities. At the Secudium Center, which oversees SK Shieldus's remote monitoring services, a proprietary Rule Framework utilizing the MITRE ATT&CK framework has been integrated into the monitoring platform "Secudium v2.0." The implemented framework is structured into nine stages within major categories, adopting a detection strategy that classifies collected information into essential and optional data. This approach allows for the organic application of threat identification and response.



Structure of the Rule Framework

Essential info	Attack Stages	14 Stages of attack lifecycle * Based on MITRE ATT&CK
	Attack Pattern	Classification of attack types * Referencing MITRE CAPAC
	Rule Name	Name used to identify the threat
	Rule Description	Technical explanation of threat detection
	Rule Recommended	Preventive measures against the threat
Optional info	CVE-Code	CVE information related to the threat
	Reference Site	Sites for additional threat information collection
	E-DB	Exploit information related to the threat
	Detect String	Patterns(Strings) used in attack

Figure 3. Structure of the Rule Framework Applied to the Secudium Monitoring Platform

The core objective of utilizing the specified Rule Framework lies in detecting and classifying threat logs collected through this system, thereby establishing a threat response mechanism that incorporates appropriate countermeasure technologies. Furthermore, by selecting specific features of Threat Hunting, it becomes possible to proactively detect techniques employed by attackers, thereby preventing the proliferation of damage and enhancing the potential for response at the initial stages of an attack.

The key to success in information security against sophisticated cyber attacks lies in 'systematic integration and iterative improvement.' From this perspective, defining a detection methodology utilizing a Rule Framework is not merely about adding new tools; rather, it is a process of redesigning the entire security operation into a threat-centric response system. By systematically classifying and operating strategies and technologies while concurrently exploring potential recurring threats, it becomes possible to establish a "proactive security system" that stays one step ahead of the attackers.

■ References

[1] MITRE ATT&CK: https://attack.mitre.org

[2] Red Canary: https://redcanary.com

[3] Mandiant Threat Intelligence Reports

[4] Atomic Red Team: https://github.com/redcanaryco/atomic-red-team

[5] Lockheed Martin – cyber kill chain: https://www.lockheedmartin.com