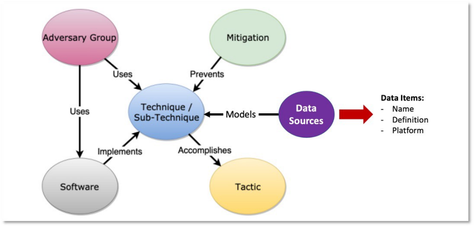
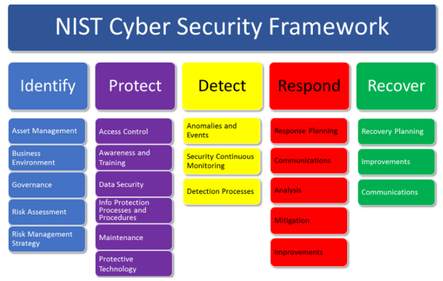
Definition and Diagram



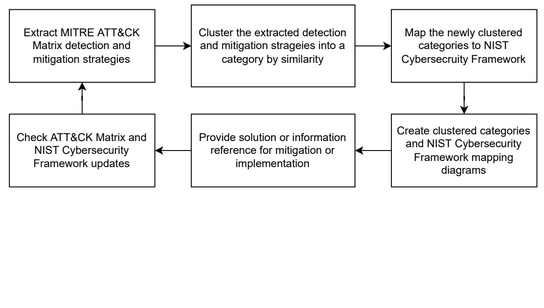
MITRE ATT&CK MATRIX

Tactic category	The adversary is trying to...	Techniques
Initial access	... to get into your network	11
Execution	... to run malicious code	34
Persistence	... maintain their foothold	62
Privilege escalation	... gain higher-level permissions	32
Defense evasion	... avoid being detected	69
Credential access	... steal account names and passwords	21
Discovery	... figure out your environment	23
Lateral movement	... move through your environment	18
Collection	... gather data of interest to their goal	13
Command and control	... communicate with compromised systems to control them	22
Exfiltration	... steal data	9
Impact	... manipulate, interrupt, or destroy your systems and data	16
ALL TACTIC EXPLOITS		**330**

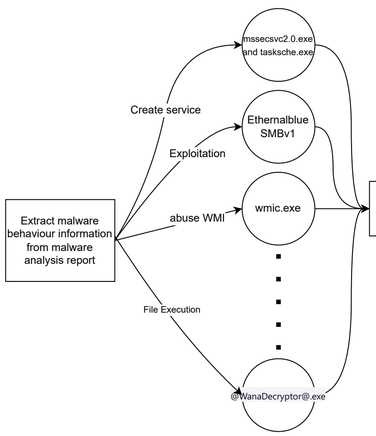


Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

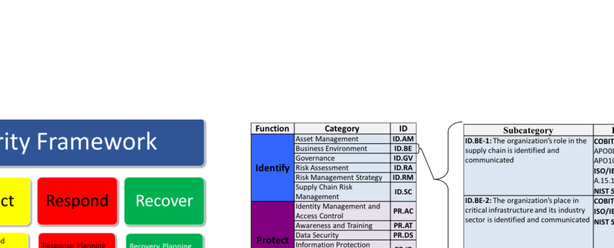


Sample in detail



Classify techniques using MITRE ATT&CK Matrix

Kill Chain stage	Technique	Description
Execution	Windows Management Instrumentation	WannaCry utilizes wmic to delete shadow copies
Persistence	Create or Modify System Process	WannaCry creates the service "mssecsvc2.0" and task schedule tasksche.exe with the display name "Microsoft Security Center (2.0) Service
...	...	...
Lateral Movement	Exploitation of remote service & Lateral tool transfer	WannaCry uses an exploit in SMBv1 to spread itself to other remote systems on a network and use SMB as a tool for copy itself
Impact	Data Encrypted for Impact	WannaCry encrypts user files and demands that a ransom be paid in Bitcoin to decrypt those files



Ransomware Defensive Profile

1	PR.AC-1 AND PR.AC-4
2	PR.DS-5 AND (DE.CM-6 OR DE.CM-7)
3	DE.AE-3
...	...

Extract MITRE ATT&CK Matrix detection and mitigation strategies

Create or Modify System Process	Mitigation	- Audit - Behavior Prevention on Endpoint - Code Signing - Limit Software Installation - Operating System Configuration - Restrict File and Dictionary Permissions - User account management
	Detection	- Command - Driver - File - Process - Service - Windows Registry
Exploitation of Remote Services	Mitigation	- Application Isoliation and Sandboxing - Disable or remove feature or program - Exploit protection - Network Segmentation - Privileged account management - Threat Intelligence program
	Detection	- Application Log - Network Traffic

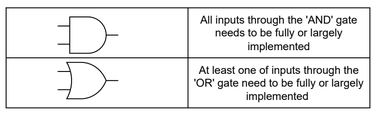
Cluster the extracted detection and mitigation strategies into a category by similarity

Category	Sub-Category
Audit	- Audit
Prevention & Protection	- Behavior Prevention on Endpoint - Exploit Protection
Validation or checksum	- Code signing
Limitation	- Limit software installation - Disable or remove feature or program
Configuration	- Operating System Configuration
Privilege & permission	- Restrict File and dictionary permissions
Account management	- User account management - Privileged account management
Intelligence capability	- Threat Intelligence program
Logging	- Command - Driver - File - Process - Service - Windows Registry - Application Log - Network Traffic

Cluster the extracted detection and mitigation strategies into a category by similarity

Category	Sub-Category	NIST Cybersecurity Framework
Audit	- Audit	(PR.DS-6 AND PR.DS-8)AND PR.PT-1 AND DE.CM-8 AND PR.AC-1
Prevention & Protection	- Behavior Prevention on Endpoint - Exploit Protection	ID.SC-1 AND ((PR.DS-1 AND PR.DS-2) OR PR.DS-4) AND PR.PT-2 AND DE.AE-2 AND (DE.CM-4 OR DE.CM-5) AND DE.CM-7
Validation or checksum	- Code signing	PR.DS-6
Limitation	- Limit software installation - Disable or remove feature or program	PR.PT-3
Configuration	- Operating System Configuration	PR.PT-3 AND PR.IP-3
Privilege & permission	- Restrict File and dictionary permissions	PR.AC-4
Account management	- User account management - Privileged account management	PR-AC-4 AND PR.AC-7
Intelligence capability	- Threat Intelligence program	ID.RA-2
Logging	- Command - Driver - File - Process - Service - Windows Registry - Application Log - Network Traffic	DE.AE-3 AND DE.CM-7

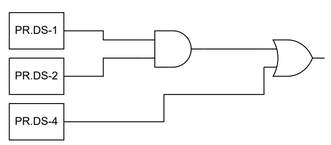
AND/OR Logic in NIST Cybersecurity Framework



All inputs through the 'AND' gate needs to be fully or largely implemented

At least one of inputs through the 'OR' gate need to be fully or largely implemented

Example: (PR.DS-1 AND PR.DS-2) OR PR.DS-4



Provide solution or information reference for mitigation or implementation

If user choose any subcategory of NIST CSF, they should go to check detail at NIST CSF Core.

For example, User choose PR.DS-3 to implementation. User go to check at NIST CSF Core and choose one standard for implementation.

PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· **CIS CSC** 1 · **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 · **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16