MITRE ATT&CK: Operationalizing the Framework to Build an Effective Cybersecurity Program

SUMMARY

Adaptive threats, increasingly demanding regulatory expectations and rapidly changing business drivers are significantly increasing cyber risks. Organizations can advance their ability to manage cyber risk by using an offense-informed-defense approach based on the MITRE Corporation's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, which was first publicly released in 2015 and has evolved significantly since then.[1] MITRE is the United States' oldest and largest operator of federally-funded research and development centers (FFRDC) and ATT&CK is the most comprehensive, authoritative approach to mapping of threat actors to tactics, techniques and procedures (TTPs) openly available today. This white paper explains how the ATT&CK framework can be operationalized to effectively manage cyber risks, including through the use of Chertoff Group Cyber Risk Diagnostic services – which apply to the core analytic approach described below - and ServiceNow Security Operations Solutions.

ATT&CK IN USE

In managing cyber risk, organizations are confronted with the following questions:

- Based on our business profile, what should we consider as reasonably foreseeable threat actor interest in my organization?
- How could threat actors actually compromise our environment?
- Does our security approach provide reasonable coverage against this kind of threat tradecraft? How do we weigh tradeoffs in alternative security investments we are considering?
- Do the security countermeasures we have in place actually work?
- If we suffer a compromise, are we prepared to respond effectively?

The ATT&CK framework helps answer these questions.

Inherent Risk Profile and Threat Model Development. The ATT&CK framework can serve as the underlying knowledge-base for an organization to consider how its business objectives influence its attractiveness to reasonably sophisticated threat actors defined in MITRE's authoritative library.

This information allows organizations to the develop a sample set of threat-actor-specific TTPs, which are referred to as a "threat model." Put another way – it enables of mapping of business profiles (for example banking and credit card processing) to threat actor groups that target these sectors (e.g., Lazarus Group and FIN 6) to impacts (i.e., subversion of payment system integrity, theft of consumer payment account numbers). Figure 1 below demonstrates how this process can work.

Figure 1 Mapping Business Profile to Threat (Financial Services Sector Example)

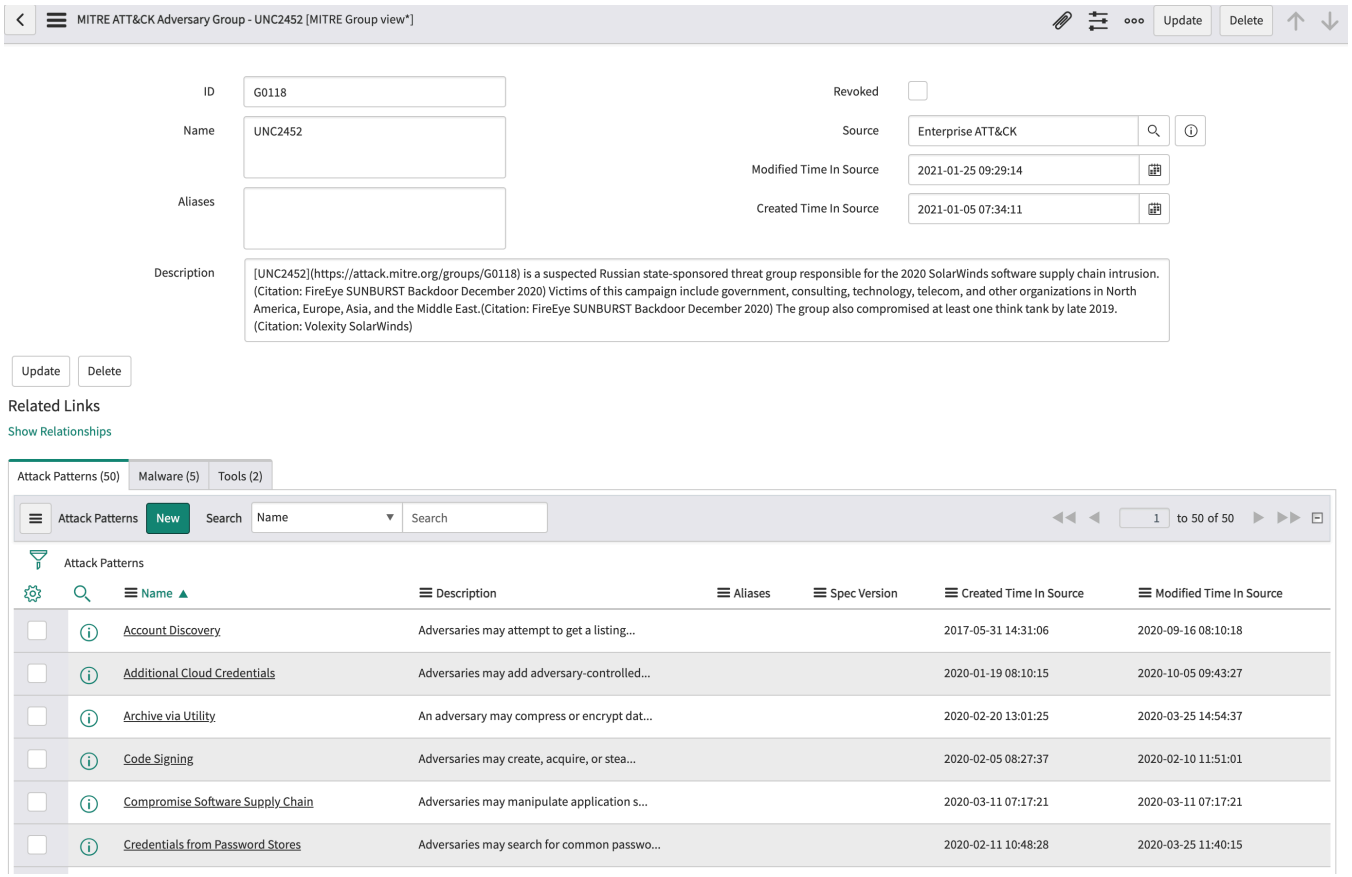
1 © 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation. More information available at https://attack.mitre.org/.

How ServiceNow helps: Inputs for this mapping may come from:

- **Business Impact Analysis (BIA) to define critical services/functions and related key business attributes.** BIAs are developed and maintained within ServiceNow's Business Continuity Management application, which has a natural integration with ServiceNow's Security Operations applications.
- **Reporting from cyber threat intelligence sources (government, commercial, open source).** The Threat Intelligence module in ServiceNow's Security Incident Response (SIR) application supports STIX 1.X and 2.X data models. The Threat Intelligence module can be integrated with many OSINT and Commercial Threat Intel feeds.
- **Incident response reporting for previous incidents, especially when categorized by TTP.** SIR captures and categorizes incident response details by TTPs as described in more detail in the "Incident Response Planning and Resiliency" section below.

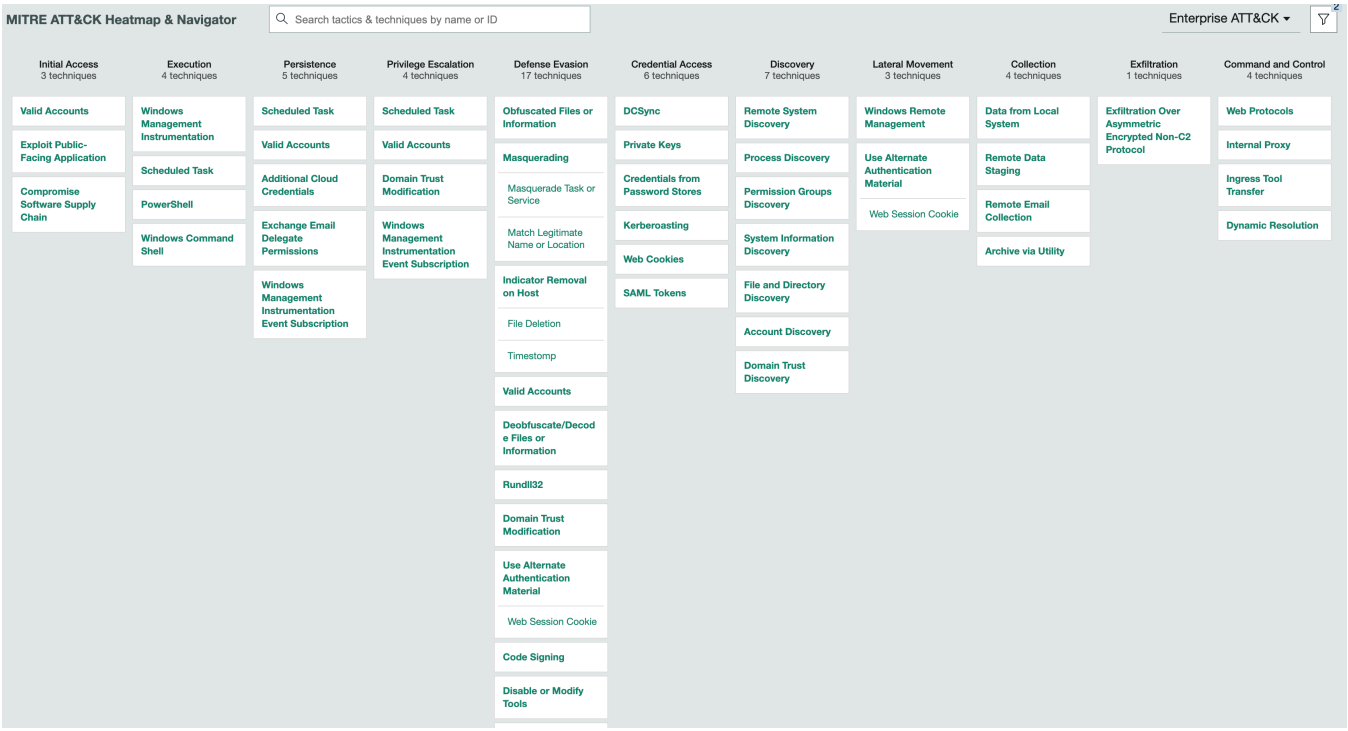
Threat model mapping using Security Incident Response. The Threat Intelligence module in Security Incident Response includes support for the MITRE ATT&CK framework. Threat Intel Analysts can analyze threat intelligence data within SIR. Security teams can map TTPs to Threat Actors. SIR's Case Management module allows security teams to create new cases based on 'Threat Actor' profile or 'Campaigns', as depicted in Figure 2 below. Artifacts like incidents, observables, IOCs, users, and configuration items can be added to the Threat Intel cases for deeper investigation.

Figure 2: Adversary Profile



Adversary behavior can also be viewed in the form of a threat pathway or "kill chain" threat model view using the Security Incident Response MITRE ATT&CK Navigator and heatmap, as depicted in Figure 3 below.

Figure 3: Threat Model View



Mapping to Defensive Countermeasures. Organizations can next map their current defensive countermeasures to TTPs identified in their newly-developed threat models. By overlaying a coverage map with a threat model, defenders gain an understanding of what technologies and standards applied in their environments are potentially addressing what TTPs. The ATT&CK framework provides a mechanism to support this mapping through the "data sources" and mitigations ascribed to each TTP contained in the ATT&CK framework.[2]

Notably, not all relevant threat techniques represent the same level of risk, and additional open source and proprietary data sets can be leveraged to prioritize TTPs based on risk reduction value. Key input factors include ease of attack, difficulty of defense and other organization-specific considerations.

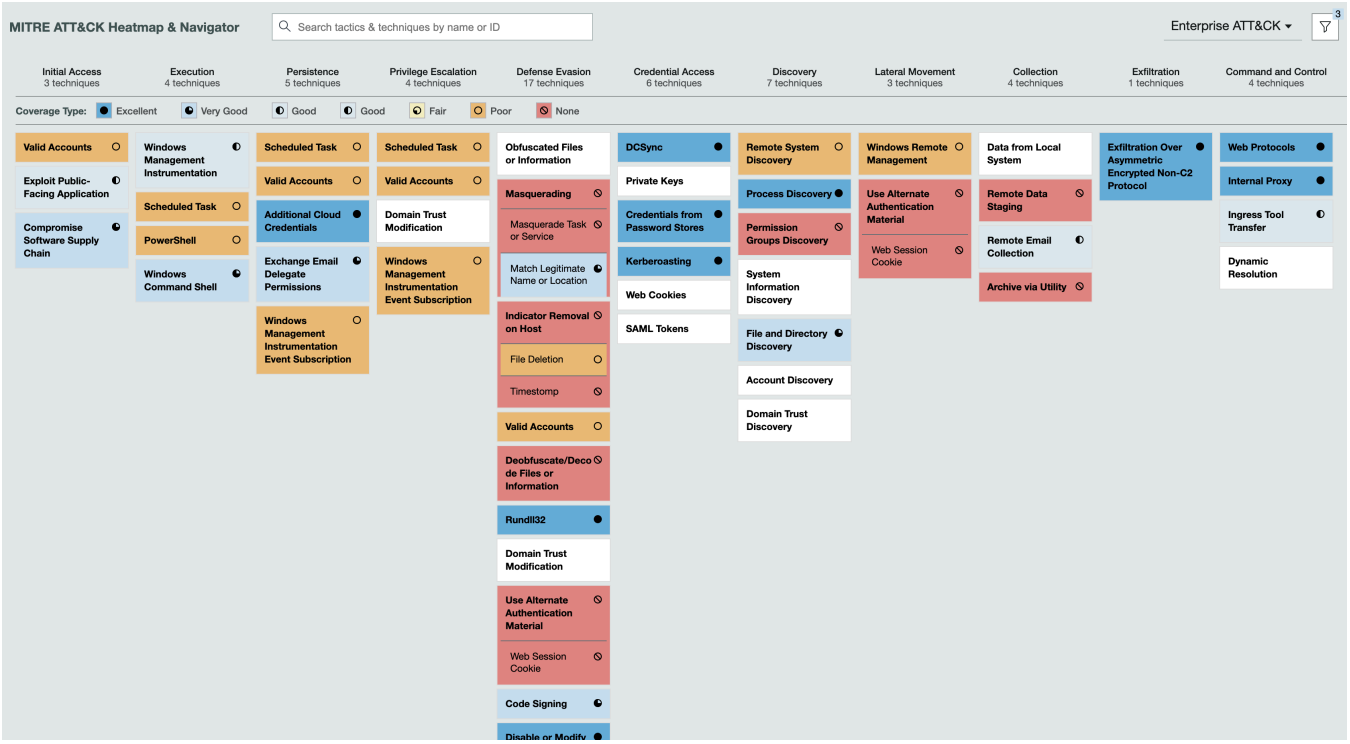
Ultimately, the TTP-coverage map also gives a defender the capability to prioritize future, defensive countermeasure investments based on risk reduction value. The data adds further depth to the overlays we just described: now, we can not only see whether a countermeasure provides broad coverage against TTPs, but also the extent to which it covers critical or high priority TTPs.

How ServiceNow helps: By mapping TTPs in ATT&CK to data sources and detection tools, ServiceNow Security Operations allows organizations to identify which attack techniques are relevant to them, prioritize the impact, assess how well they can detect and respond to attacks, track progress and measure improvement, and create visualizations for teams managing that effort and executives who need to be provided metrics.

- ***Gaining visibility into detection and response coverage of the organization on the attacker techniques.*** ServiceNow Security Incident Response has an out-of-the-box feature that supports mapping of 'data sources' and 'detection tools' to MITRE ATT&CK TTPs, as described in Figure 4 below. Detection coverage for the techniques used by relevant adversaries can be viewed in the form of a heatmap. This gives visibility into the security posture of a company against the targeted attacks by known adversaries.

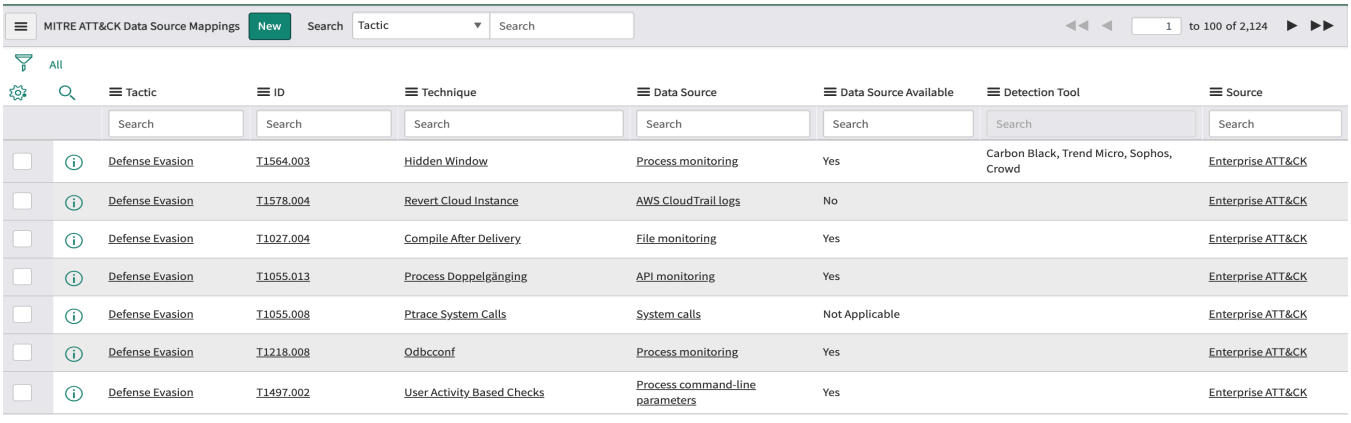
2 This overlay can also, in principle, be mapped to authoritative frameworks, and MITRE's Center for Threat Informed Defense has recently released an authoritative mapping to NIST Special Publication 800-53. See: https://medium.com/mitre-engenuity/security-control-mappings-a-bridge-to-threat-informed-defense-2e42a074f64a.

Figure 4: Threat Model View – Detection Coverage Mapping and Rating



This exercise gives visibility into event data sources, their relevance to an organization, and helps identify gaps in the coverage. Figure 5 below describes a table view of how data sources are correlated to TTPs. Organizations can enhance their environment by investing in collecting the right data sources for the right threats, and in optimizing or acquiring related detection tools.

Figure 5: Table View – Data Source to TTP Correlation



Tactic	ID	Technique	Data Source	Data Source Available	Detection Tool	Source
Defense Evasion	T1564.003	Hidden Window	Process monitoring	Yes	Carbon Black, Trend Micro, Sophos, Crowd	Enterprise ATT&CK
Defense Evasion	T1578.004	Revert Cloud Instance	AWS CloudTrail logs	No		Enterprise ATT&CK
Defense Evasion	T1027.004	Compile After Delivery	File monitoring	Yes		Enterprise ATT&CK
Defense Evasion	T1055.013	Process Doppelgänging	API monitoring	Yes		Enterprise ATT&CK
Defense Evasion	T1055.008	Ptrace System Calls	System calls	Not Applicable		Enterprise ATT&CK
Defense Evasion	T1218.008	Odbcconf	Process monitoring	Yes		Enterprise ATT&CK
Defense Evasion	T1497.002	User Activity Based Checks	Process command-line parameters	Yes		Enterprise ATT&CK

The solution can be also extended to map the defensive countermeasures based on risk reduction value.

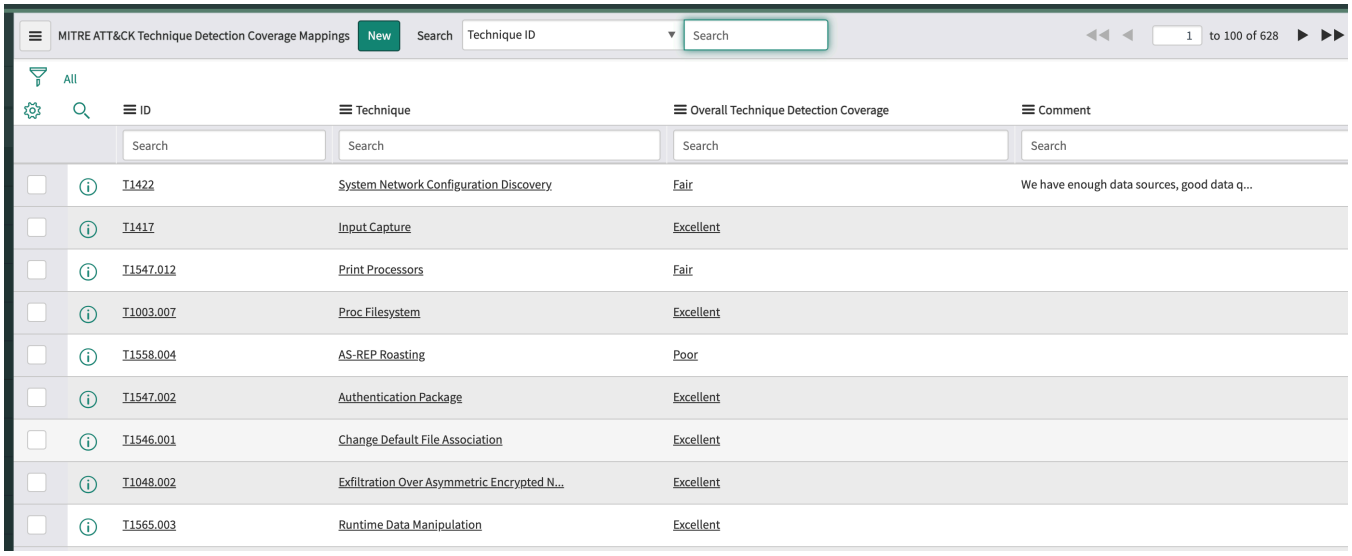
Detection Assurance Testing. There is often a lack of clarity on what types of threat activity a defensive measure actually addresses, particularly depending on how it is configured and implemented; thus organizations can meaningfully strengthen their programs by validating the extent of protective and detective capabilities' performance against simulated threat activity. Testing scripts have already been developed specific to each of the MITRE ATT&CK techniques, and these scripts can be leveraged to validate and hone defenses.

Security teams can use third-party services, automated testing tools or Breach and Adversarial Simulation (BAS) products to test their defenses. BAS tools are now available that can run TTP-specific diagnostics on an organization's technology stack. This process enables organizations to continuously validate that security controls are operating effectively, and to reveal unknown weaknesses like misconfigured security controls, unknown vulnerable assets, or ambiguous detection rules that need attention. The outcome of the exercise also reveals the overall technique detection coverage, prevention, and defensive capabilities.

- To implement testing, an organization can select a sample of assets/images that reflect both "crown jewel" considerations and machines that may be representative of IT environment as a whole. The diagnostic assessments would be conducted on these sample sets.
- We now have both really precise data on countermeasure coverage (based both on breadth and criticality of TTPs addressed) and really accurate data on countermeasure performance (TTP-specific pass/fails on testing). Using math, this data can be converted into weighted numerical values (a low value TTP might be a "3" where a high priority TTP might be a "10"). Results can then be aggregated to generate an overall risk score – for example (A-F, 0-100, 300-850, etc.). Results can be tracked over time to generate performance data and trending insights.
- It is also possible to generate reporting that demonstrates the potential positive impact of investment in a tool or standard on security performance. Such insights are invaluable when considering the costs and benefits of future security investments.

How ServiceNow helps. Organizations can reflect test results in ServiceNow's MITRE ATT&CK 'overall technique detection coverage' mapping feature, described above in the "Defensive Countermeasures" section above. As described in Figure 6 below, coverage can be classified as Excellent, Fair or Poor.

Figure 6: Detection Coverage Effectiveness Classification



Improve red team/blue team collaboration and ROI. The combination of the ServiceNow Security Operations Platform and MITRE ATT&CK Framework provides a template for collaboration. Red team members can test against specific tactics and techniques or emulate a known threat actor while blue teams have the right visualization into controls and data sources to isolate areas that need improvement. By working with the same tools and models, organizations gain visibility to granular changes for risk mitigation, and this knowledge can also help guide security investments and improve ROI on security spending.

Incident Response Planning and Resiliency

In order to achieve resiliency, organizations need to be able to effectively anticipate, withstand, recover and evolve from attacks. The ATT&CK framework helps advance resiliency capabilities in several key ways:

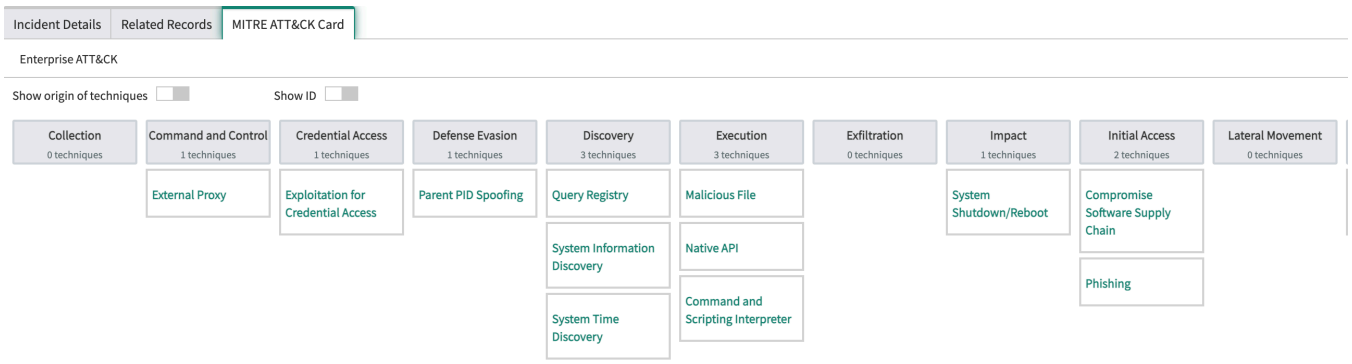
- First, ATT&CK can help prioritize response-oriented planning – e.g., to anticipate specific Lateral Movement and Privilege Escalation techniques, and to withstand specific Defense Evasion techniques.
- Second, the ATT&CK framework can also be used to categorize incidents that do occur by specific technique, which can in turn enable more focused remediation and lessons-learned activities.
- Third, ATT&CK now enumerates a specific Impact tactic which can inform incident response, business continuity and disaster recovery plans and playbooks. According to MITRE, the Impact tactic includes techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes, including the destruction or tampering of data.[3] It was introduced in part to capture disruptive behavior such as ransomware and denial of service attacks that are not captured by the other ATT&CK tactics. We can use these insights to plan, implement and maintain impact-oriented countermeasures (back-up and restore functionality, fraud control measures, etc.).
- Likewise, to help mature incident response and crisis management capabilities, cybersecurity exercises can be utilized to offer a safe environment to stress test incident response and broader security capabilities.

How ServiceNow Security Incident Response integration with MITRE ATT&CK can help SOC teams achieve IR and resilience objectives

Security professionals are taught to "think like the enemy" by envisioning the tactics and techniques hackers might employ if they were attacking an organization. ServiceNow Security Incident Response integration with the MITRE ATT&CK Framework can help achieve this goal by enabling the SOC team to use the MITRE taxonomy to inform detection and responds to adversarial behavior.

As described in Figure 7 below, security analysts can record adversary Tactics and Techniques into Security Incidents and visualize them in the MITRE ATT&CK card.

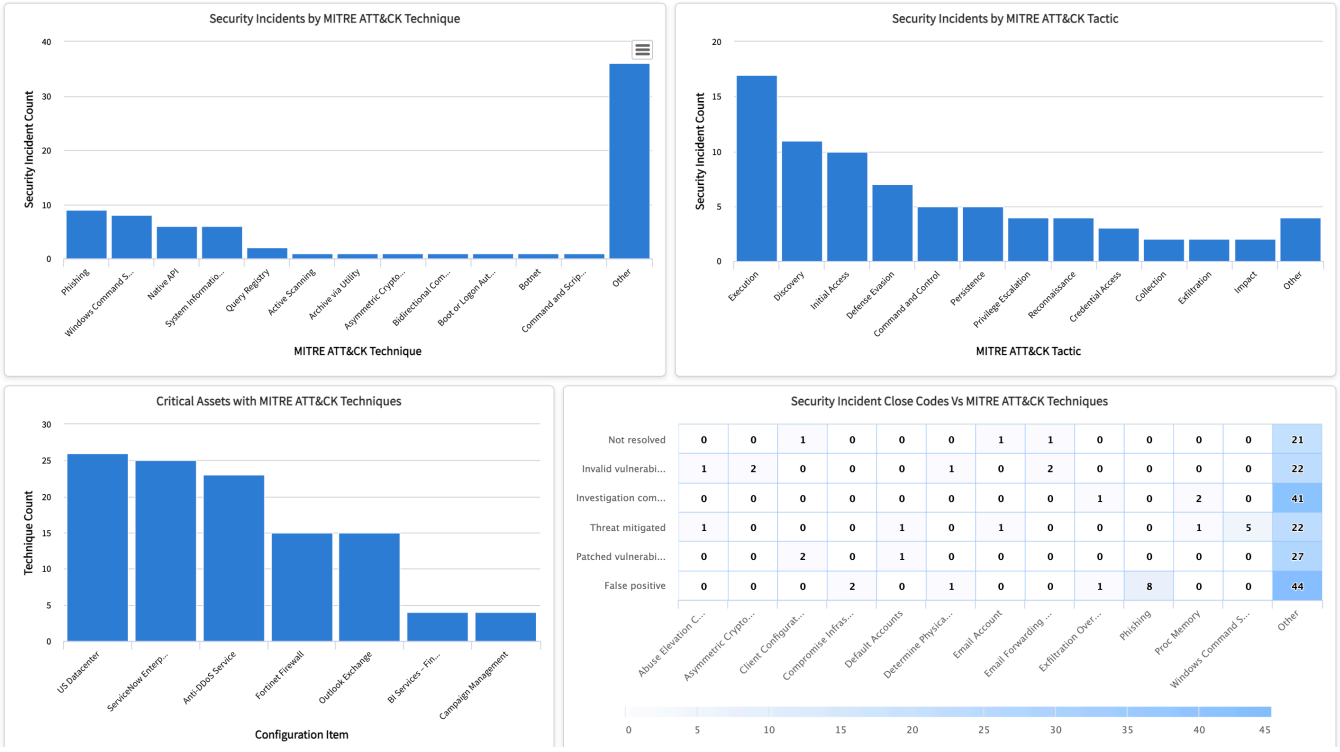
Figure 7: ATT&CK Characterization in Security Incidents



3 *See, e.g.,* ***https://attack.mitre.org/tactics/TA0040/***

- Equipped with the MITRE ATT&CK context, security analysts can respond faster to security threats using playbooks. Playbooks can be built easily in Security Incident Response using 'low code/no-code' flow designer tech stack.
- MITRE ATT&CK specific filters and the MITRE ATT&CK navigator in Security Incident Response can be used for correlating on-going and past threats in the context of MITRE ATT&CK to see if a more sophisticated attack is in play that otherwise would have gone undetected.
- Out-of-the-box widgets also provide insights about the top techniques and tactics seen in an organization's environment, as described in Figure 8 below.

Figure 8: TTP Sightings within the Organization



TARGET OPERATING MODEL CONSIDERATIONS

ATT&CK provides a common language around threat to help align internal stakeholders with direct or indirect cyber defense responsibilities – e.g., security engineering, incident response, risk, business continuity and disaster recovery and related functions, as notionally described further in the table on the following page (specific roles will vary in each organization). In other words, ATT&CK provides stakeholders a more precise means of clearly defining known adversarial tradecraft and the state of an organization's cyber defenses against that behavior.

ATT&CK also provides the building blocks for sector-level threat models that could, for example, be developed and maintained by sector-specific Information Sharing & Analysis Organizations (ISAOs).

Key Roles	Key Questions	How ServiceNow Security Incident Response, Chertoff Cyber Risk Diagnostic and MITRE ATT&CK help
Inherent Risk Profile		
• **Business Line** • **Chief Risk Officer (CRO)** • **Chief Information Officer (CIO)** • **Chief Technology Officer (CTO)** • **Chief Information Security Officer (CISO), Audit** • **ISAO**	• Based on my business profile, what should I consider as reasonably foreseeable threat actor interest in my organization? Which assets are most likely to be targeted?	• Ability to map business profile to ATT&CK threat actor groups based on known interest in similar business profiles
Threat Model		
• **Threat Intelligence Lead** • **SOC** • **ISAO**	• How could threat actors actually compromise my environment?	• Ability to map relevant threat actor groups to TTPs • Ability to add known incident TTPs to threat model • Ability to add TTPs reported in cyber threat intelligence reports to threat model
Defensive Coverage Map		
• **Security Architecture & Engineering** • **SOC** • **CISO/CRO** • **CIO/CTO**	• Does my security approach provide reasonable coverage against this kind of threat tradecraft? How do I weigh tradeoffs in alternative security investments I am considering?	• Ability to map ATT&CK TTPs to data sources (via OOTB functionality) • Ability to map ATT&CK TTPs to mitigations and controls • Ability to evaluate relative coverage ROI for specific TTPs, data sources and mitigations
Controls Assurance		
• **Security Architecture & Engineering** • **SOC** • **Audit** • **CISO/CRO** • **CIO/CTO**	• Do the security countermeasures I have in place actually work?	• TTP-specific tests on assets based on risk can be done using internal expertise and third-party cybersecurity products and services • Results can be presented in Security Incident Response
Incident Response & Resiliency		
• **SOC** • **Business Continuity/ Disaster Recovery** • **CISO/CRO** • **CIO/CTO** • **Business Line** • **ISAO**	• If we suffer a compromise, am I prepared to respond effectively?	• Ability to map incident response actions to TTPs and impacted assets • Ability to reflect ATT&CK impact-oriented techniques into defensive strategy • Ability to seed exercises with relevant TTPs

Security teams have been historically challenged in internalizing an adversary's intent and tradecraft both architecturally and when dealing with security incidents, and may incorrectly prioritize security incidents without this insight.

Now, with this new capability, threats and incidents are mapped to the MITRE ATT&CK framework to provide advanced context on attacks. This enables analysts to stay ahead of attackers and reduce the overall attack surface. Likewise, once a security incident is mapped to a MITRE tactic or technique, security analysts can use the ServiceNow ATT&CK Navigator to visualize how an individual tactic or technique is used by the numerous adversaries tracked by MITRE. Security analysts now gain an adversary perspective and a roadmap for investigations, resolution and after-action analysis.

WANT TO LEARN MORE ABOUT HOW SERVICENOW SECURITY OPERATIONS HAS LEVERAGED THE MITRE ATT&CK FRAMEWORK? REFER TO THE PRODUCT DOCUMENTATION.

WANT TO LEARN MORE ABOUT HOW THE CHERTOFF GROUP HAS OPERATIONALIZED MITRE ATT&CK? REFER TO INFO@CHERTOFFGROUP.COM

servicenow

TheChertoffGroup