MITRE ATT&CK

Framework and Its Impact On

Security Operations

(Focused on RBA)

DATE : 20th Nov 2022

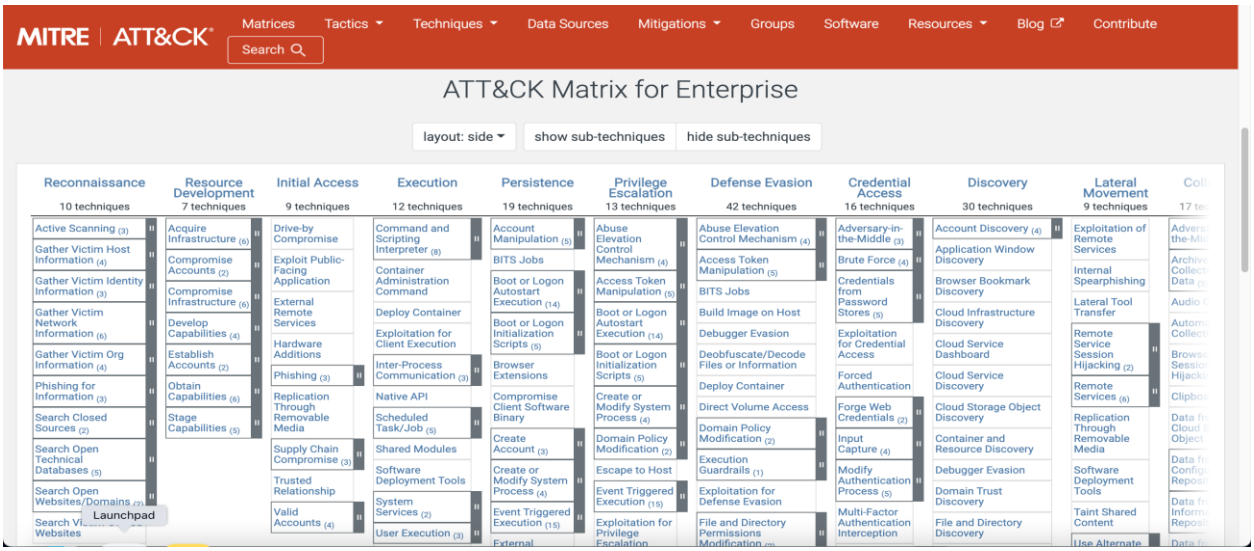
AUTHOR: Suprith D Raj

Table of Contents

MITRE ATT&CK

MITRE Corporation, a not for profit organization has developed and maintaining the ATT&CK framework. It is a library of Adversarial Tactics, Techniques and Common Knowledge. This framework also contains information about the Adversary groups, Software and tools used by specific adversaries, detection and mitigation techniques.

What is MITRE ATT&CK?



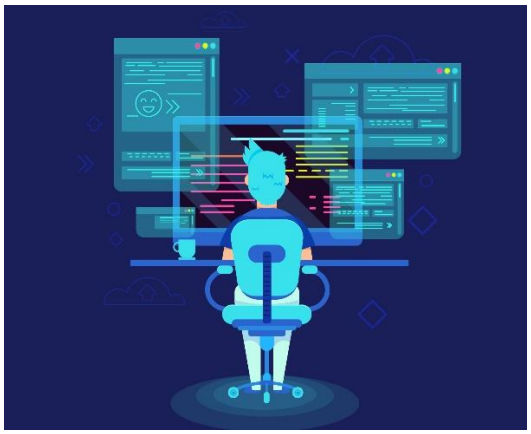
The ATT&CK metrics contains the tactics, which are the set of goals that the adversaries are trying to achieve. And the techniques are the different ways or mechanisms using which the adversaries can achieve those goals. This gives a detailed view of an adversary behavior though out the attack cycle.

By analyzing this behavior and correlating it with the data gathered in an incident, the SOC analysists can answer the Who, How, What and Whys of a particular security incident. In this way ATT&CK framework can substantially decrease the incident response time. There are several other advantages which will be discussed in this report.

How to Use ATT&CK Framework?

Let us take a simple case of a Patient visiting a Doctor regarding an infection which he has caught with. So the Doctor observes the patient's external, internal symptoms and behaviors. Once he has completed his observation, he will look though the knowledge base which he has gathered over several years of experience to correlate his observations with the similar behaviors of pathogens in his knowledge base. Then the doctor will diagnose the infection. Doctors lets the Patient know, ***which*** pathogen might have caused the infection, ***How*** the pathogen might have entered in to the patient's body, ***What*** does

the pathogen do to the body, ***How*** to get rid of the pathogen and ***How*** to detect similar infection in future.



Similarly, ATT&CK framework is a knowledge base of adversarial behaviour gathered from different data sources and contributors over a long period of time. Analysts can use this library of adversarial behaviour to

- Answer the questions like what do the adversary want to achieve, how they would achieve those goals, which path they would take to achieve their goals, which tools they could use, how to detect those attacks and how to mitigate those attacks.
- Build a Risk based Alerting model
- Develop a mature threat model
- Faster incident response
- Better preparedness for any future attacks

Things to Note While Using ATT&CK Framework

There are few things, as a security analyst or any cyber security person should not before using ATT&CK framework. It is crucial to know these points since these could have a direct impact on design, implementation and cost of the security model. Ignoring these could also result in poor security implementation and increase attack surface.

1. ATT&CK framework is not a checklist which you can mark as completed after implementing mitigation for adversaries in the framework. A security model might have implemented the ATT&CK framework completely, but it doesn't mean that they are completely covered. It only provides a better security posture.
2. ATT&CK framework also consists of commands which can be run as mitigation techniques, but beware not to use those commands before completely understating that it is actually doing. Especially in production environments.
3. Do not assume that the ATT&CK framework is complete and if you have implemented it, you are completely covered. The framework keeps evolving. New TTPs will be keep adding and modified always.

4. Make sure to use other knowledge base and frameworks also, like NIST Cyber Security Framework, OWASP Cyber Defense Matrix
5. Note that it is just a baseline of adversarial behavior and do not assume that the adversary behavior will be exactly the same. Adversaries are also evolving over time and coming up with new tactics and techniques.

Ways to access ATT&CK Framework

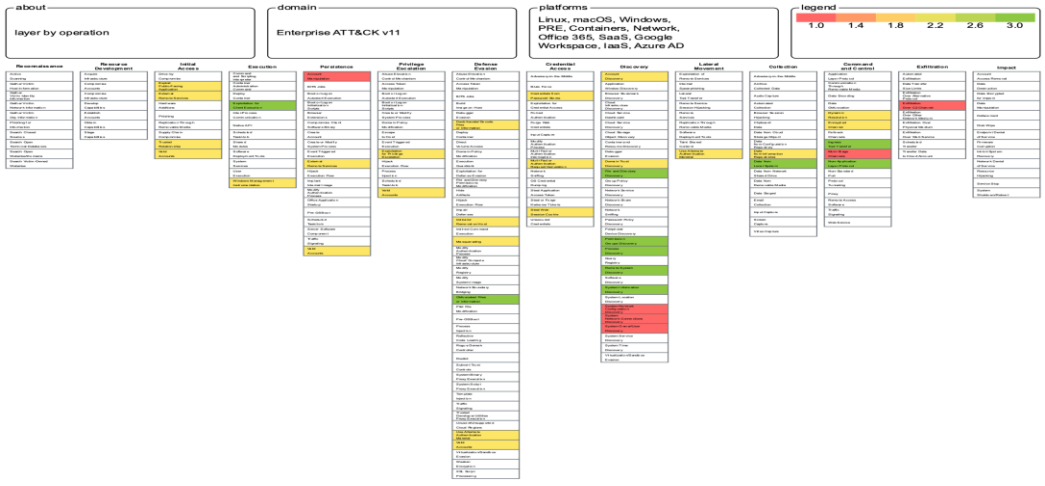
1. Accessing ATT&CK Data
    a. ATT&CK in STIX
    b. ATT&CK in Excel

2. Tools for working with ATT&CK
    a. ATT&CK Navigator
    b. ATT&CK Workbench

3. Programmatically access ATT&CK
    a. ATT&CK Python Utilities

ATTT&CK Navigator

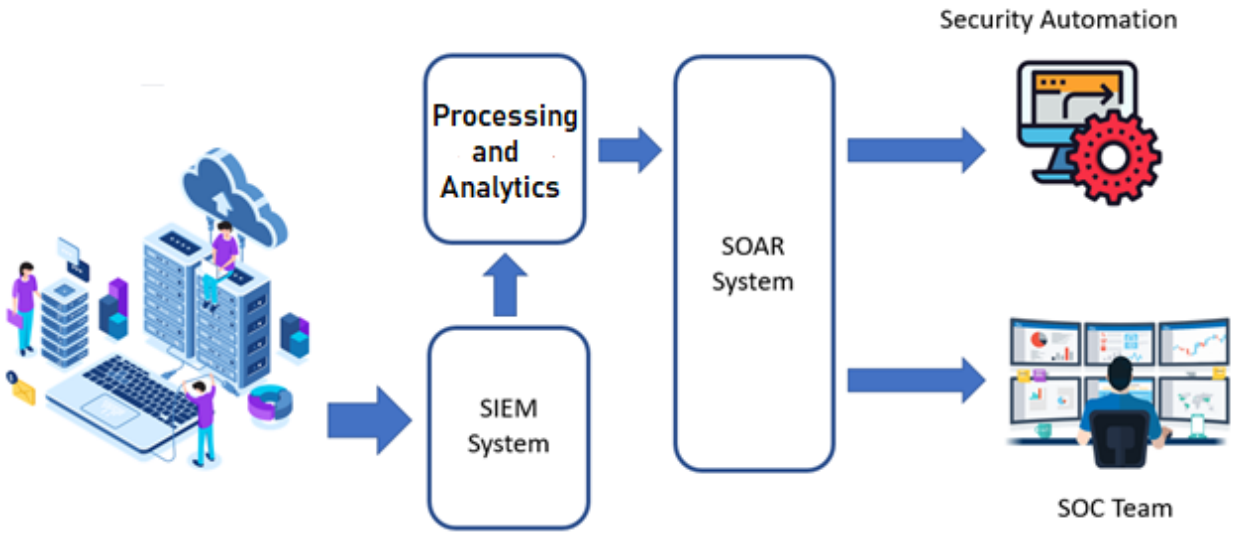
ATT&CK Navigator is basically designed for anyone who would want to put their security coverage in the form of a heat map. Using the feature of layers, one can create different layers for individual adversary emulation or based on infrastructure components or any other available filter. Options are also available to correlate between the layers to visualize as per out need. Like the one in below screenshot, a heat map is generated using the navigator which correlates the adversarial behavior of two separate adversaries, the common tactics and techniques used by those two adversaries is highlighted in green and that of individual are represented by yellow and red respectively.



ATT&CK in SOC

Scenario without ATT&CK in SOC

In a normal SOAR system in the below diagram we can see how the log data from an IT infrastructure is traversed through multiple systems to finally reach the SOC analyst in the form on an alert or incident. The SIEM software collect this huge inflow of log data in real time, normalize and correlate the data and generates alerts to the SOAR systems based on the insights gathered from analyzing the events. All these alerts are pushed to the SOC analysts or automated software is employed to take automatic action on each of those alerts based on the predefined rules. This will create an overwhelming workload on the SOC Analysts since they have to deal with a huge flood of alerts, with less or no idea about which one poses more risk on the system and should be prioritize. This will create, what they call it as alert fatigue. Alert fatigue not only affects human analysts, but automated software systems too. Resulting in unnecessary resource consumption, slowness and even breakdown in the case the scaling of the system resources is not taken care of.

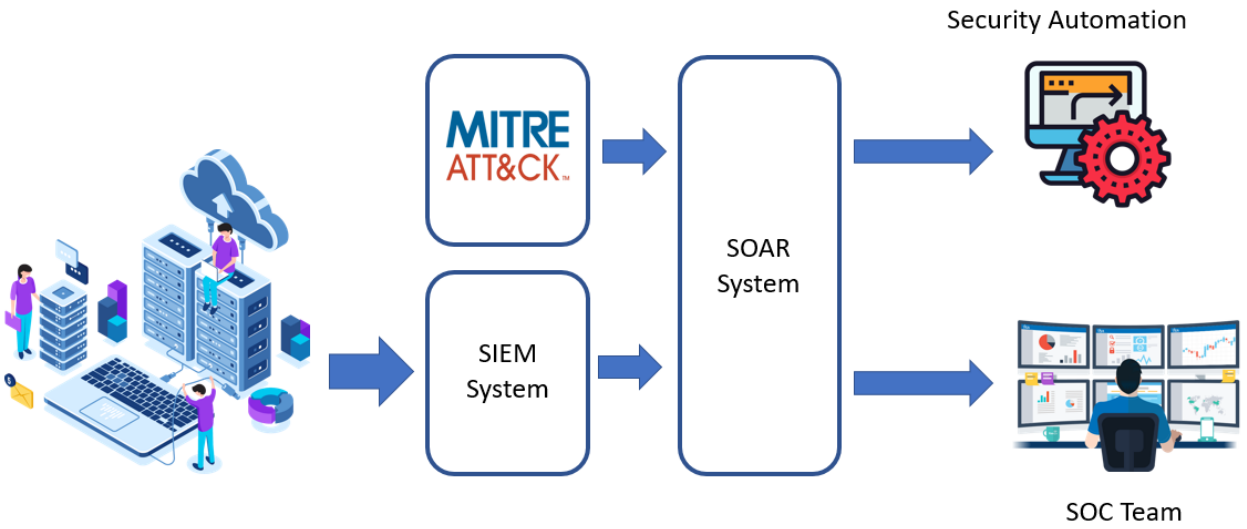


So it becomes essential to systematically handle this scenario of alert fatigue. There should be some measurement done to say, which assets or individuals are at more risk and what should be the priority that has to be set for the alert.

Scenario with ATT&CK in SOC

ATT&CK framework has a very wide range of usage. It is used across many teams dealing with cyber security. Penetration testers and Red teamers will use this framework for automated adversary emulation and simulate the tactics and techniques used by a particular adversary group on live systems. This gives them a clear visibility of where the doors are open for attackers.

However Blue teamers like the SOC analysts use this framework for variety of reason ranging from developing threat model, alerting model to incident response.



Using MITRE ATT&CK framework and based on the asset or user being affected, a Risk value can be generated. The ATT&CK tactics, techniques and the adversarial behaviors play a major role in arriving at a risk value. The risk value is then attacked to the asset or user. Based on this risk value, the priority of the incident can be clearly defined. There are other factors that also influence the risk value.

- Who is using the asset
- Number of Assets affected
- Are those assets of same type or different.
- Number of user affected
- What privileges does the user have?
- Whether the asset is internal or internet facing
- What data does the asset hold?
- How bad is it for the smooth operation of business?

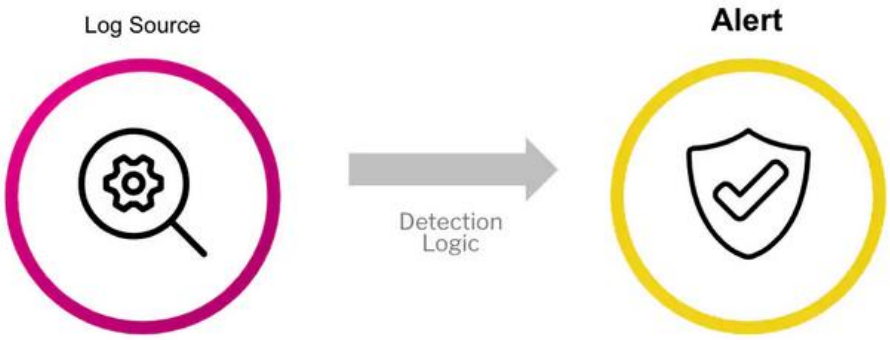
In this way an extra layer of abstraction is achieved using which SOC analysts can overcome alert fatigue and concentrate on the assets and users with higher priority. This

also helps in grouping similar alerts generated from multiple assets of users, together and bundle them in to a single incident.

Risk Based Alerting (RBA) with ATT&CK Framework

During a typical day of a SOC Analyst, there will be an overwhelming number of alerts that are generated for different assets and users. Each time the analyst has to search through multiple sources to collect necessary information for the analysis of the suspicious activity. Even for false positives, the process remains same until it is determined that is actually false positive. This is a very cumbersome process and creates alert fatigue. Also, not having sufficient information to prioritize the alerts creates an extra overhead on the analysts.

In a typical Alerting system. It takes the logs from IT infrastructure, apply predefined detection logic and generate an alert for the event which comes in to the positive purview of the detection logic.



To mitigate scenarios like above, the industry is quickly adapting Risk Based Alerting (RBA) Technique. With RBA, instead of directly generating alerts, insights are extracted by analyzing the output of detection logic.

The observations made in those insights are then correlated with the security metadata from frameworks like the MITRE ATT&CK. A risk score can be assigned or the score can be tuned based on the attributes discussed here. So in this case the alert is generated only when there are enough observations that can say this is a real suspicious activity.

That being said, RBA with ATT&CK framework empowers the SOC Analysts in below ways

- Alerts are correlated with the tactics, techniques and procedures present in the ATT&CK framework and all the useful information which is required to start with, are added to the alert before pushing it to the analysts. So now, the analysts know where to look at and what to look for at the starting point.
- Different assets, users and IDs are added to different buckets in the form of risk-objects. These risk objects are then associated with threat objects like the IP address of the asset or the asset used by the user, capabilities of the said risk-objects etc. So when a series of similar alerts are generated for different risk objects with same threat-objects being used in the suspicious activity, then those alerts are clubbed together. This reduces the number of alerts drastically
- An alert generated for a risk object with only 1 threat object contributing to the suspicious activity could be a case of false positive. So before pushing it to the analysts, weightage is given to the facts like how many threat objects are involved in the activity and is that activity really being an accomplice in a real incident. RBA increases the fidelity of the alerts and most of the false positives will be filtered out.
- A risk score will be calculated and assigned to the risk objects. Based on this, analysts will be able to prioritize the incidents effectively and help in better incident response time.
- Implementation of RBA process, by its nature helps in developing a valuable library of metadata relevant to the risk objects and threat objects. Like the tactics, techniques, procedures and the entire adversarial behavior.
- Integration with ATT&CK framework can give a better coverage of risk by providing valuable information about the detection and mitigation techniques that can be used. When an Analyst has all this relevant information when the incident comes in, it saves both time and money to the organization.
- Identify gaps in security posture by looking at the spectrum of tactics and techniques which are already covered and which are yet to be covered.

RBA Implementation with ATT&CK Framework

Traditionally, the detection algorithm creates alerts based on the predefined conditions which need constant tuning. This introduces a lot of noise in to the system and the chances of false positive also increase. So when there is a new attack, the developers have to look at the detection algorithm and again make tuning taking in to consideration, all the assets users and IDs.

As an overhead to this, an analyst has to pick each event, analyze it, attack all the necessary information, assign a priority, determine the risk and then triage it to the respective SOC team. Lot of time, energy, money and compute power are wasted in this traditional approach.

So the modern SIEM and SOAR service providers who are more focused on customer success, are hardwiring the RBA capabilities to their software at the grass root level itself. Below we will see how RBA and Mitre ATT&CK Concepts are implemented.

Implementation in Splunk Enterprise Security (ES)

Alerts are generated with respect to either an asset, ID or a user displaying specific behavior or doing certain activity. So before setting risk in RBA, a thorough audit is done to make sure the valid authorizations are in place for all the users, IDs and assets which can clearly tell who can do what and what data do they hold and how can are authorized to use it.

Formula to calculate Risk Score:

$$\text{Risk Score} = \text{Risk Impact} \times \text{Risk Confidence} \times \text{Risk Modifier}$$

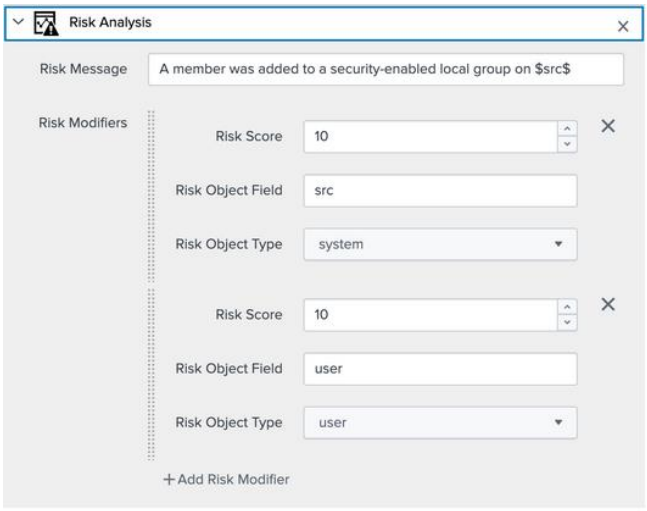
Terminologies:

- **Risk Index**: This is a repository where all the triggered alert data is stored. Like the conditions to when to generate an alert, when to consider the alert as false positive etc.
- **Risk Object**: an User, Asset or IDs
- **Risk Score:** Risk score is a number which is calculated by using three variables Risk impact, Risk Confidence and Risk Modifier
- **Risk impact**: The level of negative impact that can be caused in a particular asset, user or ID is compromised. This is basically this severity
- **Risk Confidence:** The number which defines how confident that he alert is a true positive
- **Risk Modifier:** This is a variable, like a lever which can be turned to fine tune the alerting. The risk modifier score is determined by number of factors describe here like criticality of the user or asset and the business impact.

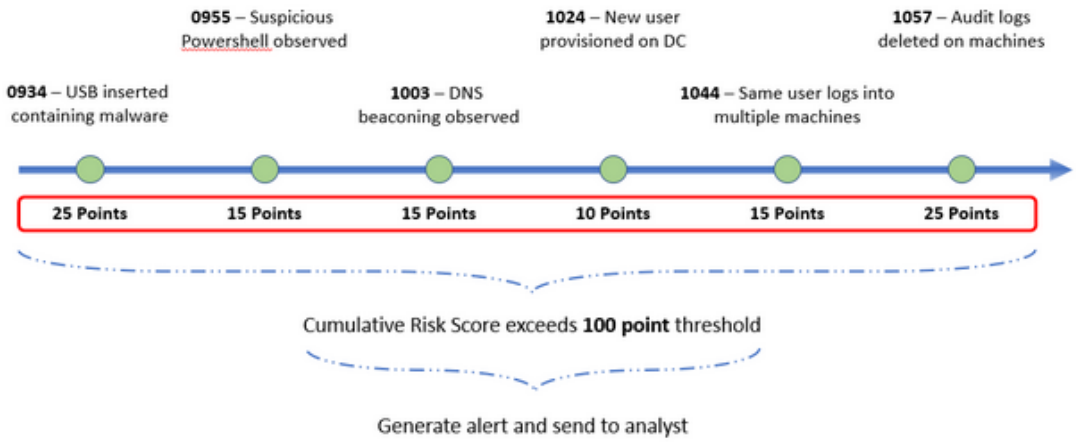
- **Risk Incident Rules (RIR):** The thresholds and patterns that are determined to be suspicious.

After calculating the Risk Score for the Risk Object, the existing Risk Index is enriched with this Risk score. The RIRs are provided by looking at the enriched Risk Index. For example:

1. There is an user whose Risk score is 10 points, and the threshold is 10%, and during an event, the risk increase to 11 points then the alert is not generated, only when it increases to 12 points the alert is generated since it crosses the threshold of 10%



2. There is an asset, say a windows machine where multiple tactics and techniques from MITRE ATT&CK framework are being executed which are observed to be specific adversarial behavior.



The bottom line is, an individual event, by itself may not contribute an event. But a set of events happening over a period of time, systematically in different areas of the infrastructure are correlated and an event is generated.

Once an even is generated the incident is assigned to the analyst. With RBA being in the system, now the analyst has 1 incident in the place of 10. The risk and priority of the event already attached to the incident, with complete security content relevant to the event from ATT&CK framework. In this way alert fatigue is reduced and a faster incident response it achieved.

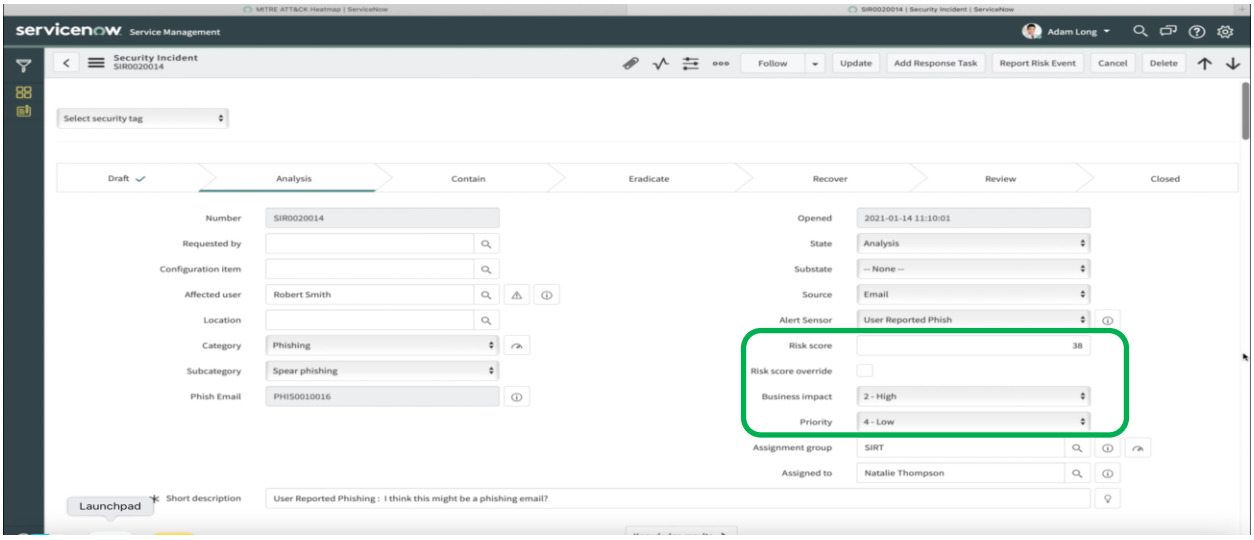
Implementation in ServiceNow Security Operations (SecOps)

ServiceNow SecOps is a proprietary software. The most targeted processes include vulnerability management and threat intelligence operationalization and how they manage and contextualize data for analysts. SecOps overlays MITRE ATT&CK TTPs on operational workflows boosts quality, structure, and consistency of security operations and enables organizations to assess their overall cybersecurity strategy and close gaps.

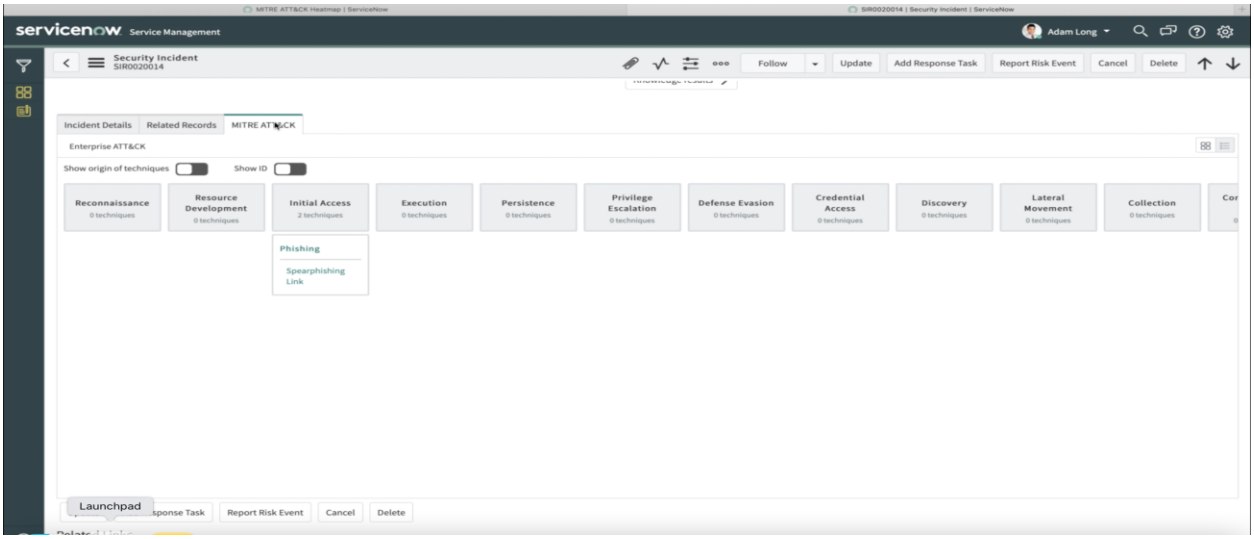
SecOps provides a platform that unifies SOAR, risk-driven vulnerability and configuration management, threat Intelligence, asset data, business context, and IT operations with the MITRE ATT&CK framework. This can help organizations address the scale, scope, and sophistication of today's threat landscape.

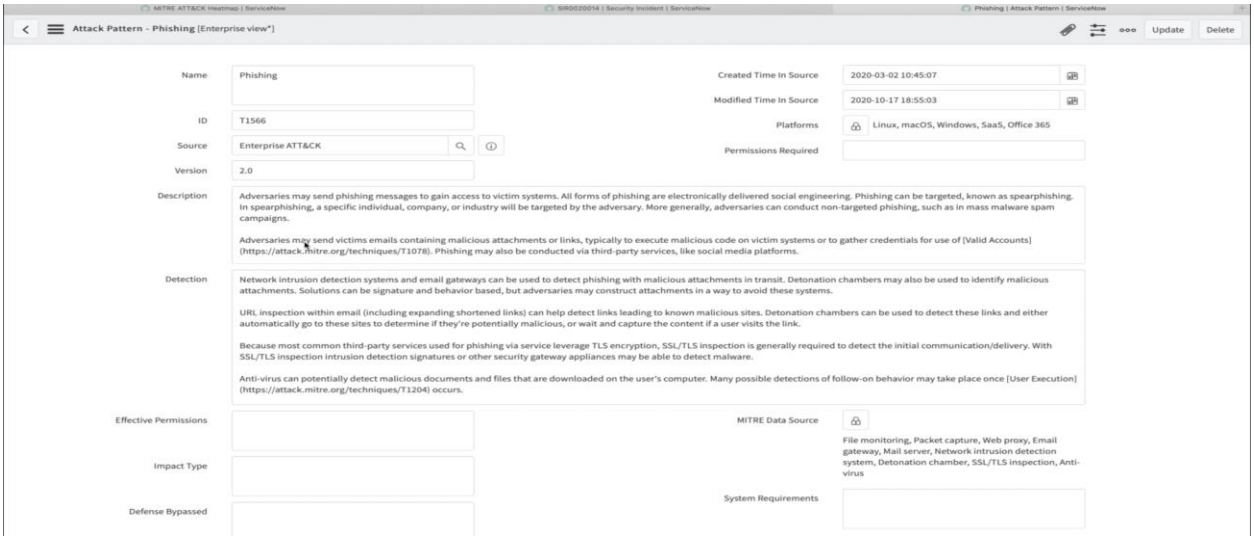
While the Splunk calculates risk based on a formula, Service now has given freedom to the customers to choose between the risk calculator plugin or customize how they would want to calculate the risk. The Risk score is basically calculated based on Risk calculator properties set by the administrator along with the Risk and impact conditions.

Example: Below incident for a suspected phishing email.

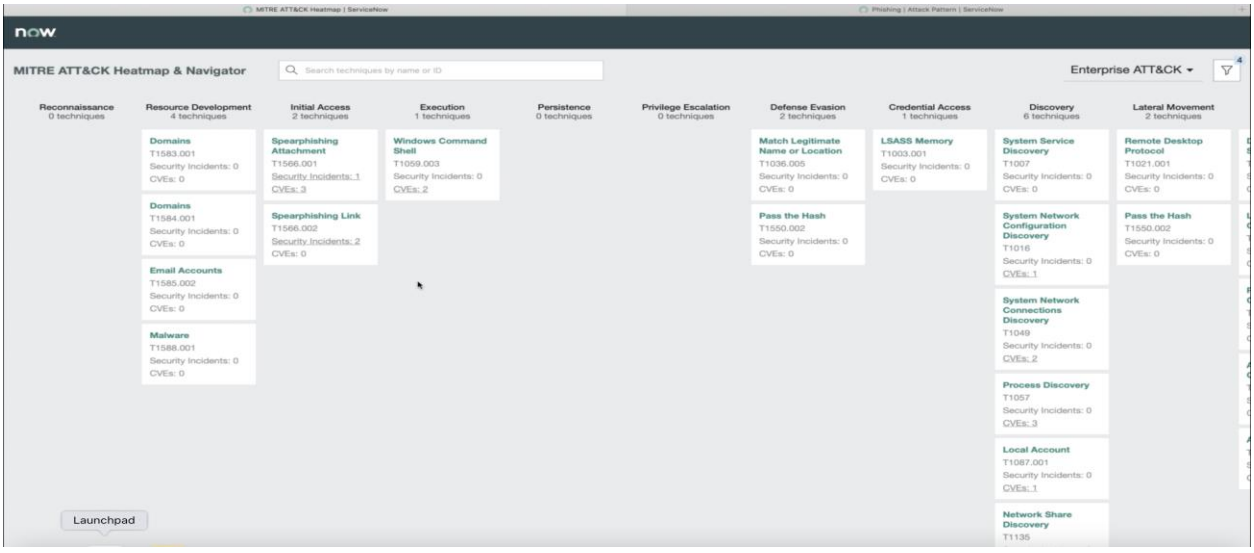


SecOps automatically pulls information from ATTACK Framework and attack it to the incident

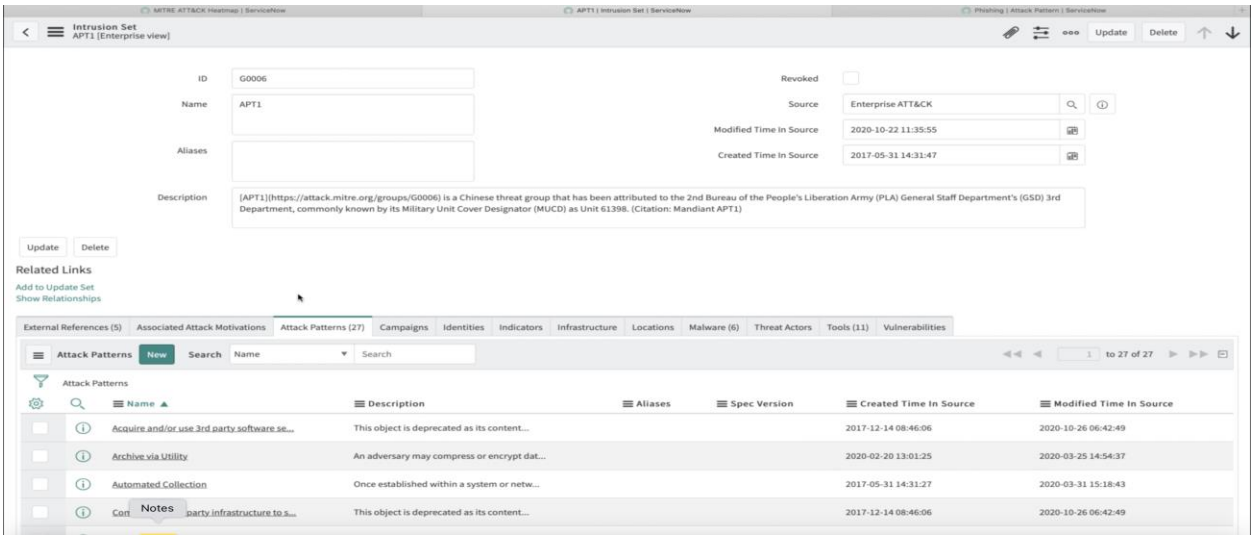




Exclusive access to ATT&CK Navigator



Analyst can also access information about the threat group whose adversarial behavior is similar to that of what is reported in the incident



The impact of MITRE ATT&CK framework on SOC (RBA) - Bottom line

SOC Without ATT&CK and RBA	SOC With ATT&CK and RBA
Analysist experience Alert Fatigue	Analyst Doesn't experience Alert Fatigue
Slower incident response	Fast and effective incident response
Manual Triaging on alerts	Automatic Triaging with minimal human effort
Less idea about security coverage	Gives clear idea about security coverage and gaps are identified
Frequent Manual tuning of the detection algorithm is needed to omit false positives	False positives are easily identified and omitted.
Analyst has less information about the incident.	Analyst will be served with all the security content present in ATT&CK framework, so that analyst can quickly analyze and respond.
Takes less time to implement	Takes more time to implement, since the changes has to be made in the cultural level in the organization

MITRE ATT&CK – Impact on Next Gen Security Operations

The Next Gen Security Operation is already here. Companies like ServiceNow have already started integrating ATT&CK framework in their security tools combined by AI and ML algorithms. The three main features of the Next Gen Security Operations in the context of ATT&CK Framework are

1. AI and ML based detection and automatic response
2. CVE to ATT&CK mapping
3. Automated Blue Teaming

Now let us look at how ATT&CK framework fit in to these advanced features that Next Gen Security Operations have to offer.

AI and ML based detection and automatic response

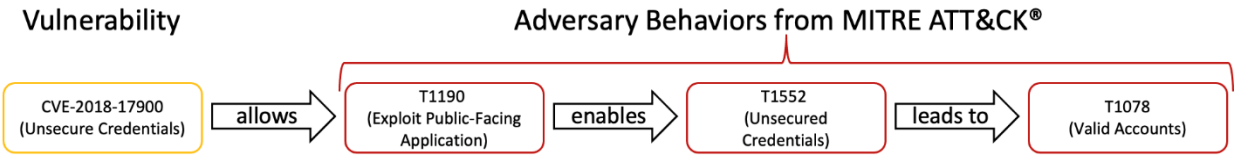
The applications of AI and ML algorithms is growing at an exponential rate in multiple sectors. Security Operation is one of those areas where the AI and ML techniques will be extensively employed. With AI and ML

- There will be minimal or no need of detection based on rules and signatures.
- AI and ML systems can learn and analyze the normal behavior of a user, entity, asset of an ID to create a profile and store it in the knowledge base.
- These systems can create a behavioral metrics for these objects similar to that of ATT&CK metrics.
- When there is a deviation from the normal behavior, based on the predefined threshold and correlating other events which are relevant, AI and ML systems can detect suspicious behaviors and generate alerts with more fidelity.
- Apart from detection and alerting. Based on the event behavior, the security content in ATT&CK framework is enriched.
- The AI and ML systems can also respond automatically based on the adversarial behavior described in ATT&CK framework. For example, if there is DDOS attack detected, AI and ML can automatically deploy mitigation techniques like blocking the port and the IP addresses involved in the attack. This will quickly stop the attack from manifesting further. Or if any application is displaying suspicious behavior, then automatically sandbox the application.

- Insider threats can be easily identified since the AI and ML logics work based on user's behavioral analysis.

CVE to ATT&CK mapping

Creating a link between CVE database and the ATT&CK Tactics and techniques has been in talks for quite some time. With the advent of Next Gen Security operations, this will become one of the most important tasks to the engineers. Making this work will add more value and information to the existing security content. The SOC analysts will have yet another efficient way of dealing with the incidents. Having more information is always a plus point and decreases the time spent in analysis, in turn promoting faster incident response. Linking these two knowledge bases helps in better correlation and to perform advanced threat hunting for better preparedness.



Let us take an example of a public facing web application which stores the login credentials in a file within its context root directory. Like shown in the above diagram, CVE-2018-17900 can be associated with this vulnerability which means unsecure credentials. Which means anyone who could traverse through the directories will gain access to these credentials. So how does it look like when mapped with the ATT&CK Tactics and Techniques? The Tactic which the adversity is trying to achieve is T1190 that is Exploit Public Facing Application. The adversaries use the technique T1552 to search the directories to gain unsecured credentials. This will lead to another technique T1078 that is valid accounts.

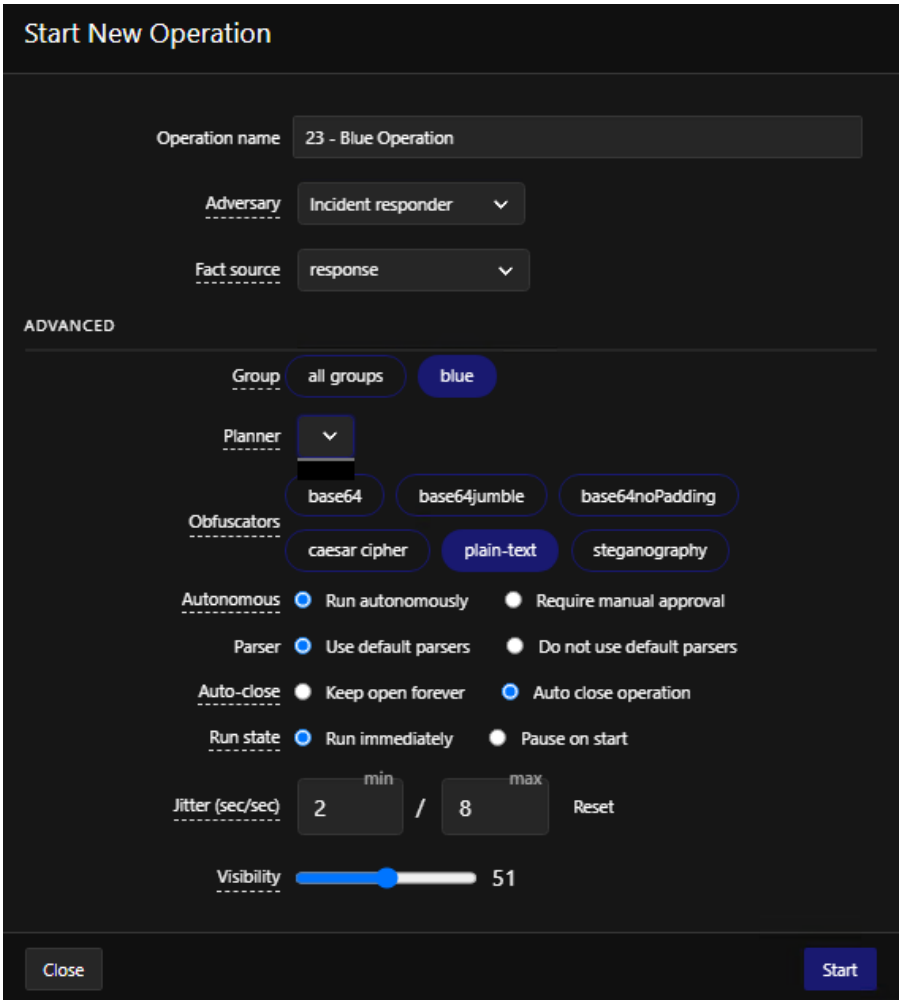
When a suspicious activity of querying root directory is observed by the SIEM software and simultaneously multiple other events of unusual logins are observed in the web application logs, the Next Gen SIEM tools can attack the ATT&CK information to the alert and at the same time based on the linkage between ATT&CK and CVE, query the CVE database and add vulnerability information to enrich the security content that is being delivered to the SOC analysts. This will give an upper hand to the analysts, and they can quickly deploy mitigation mechanisms to patch the possible vulnerabilities. This also helps in proactive threat hunting and improving the security posture.

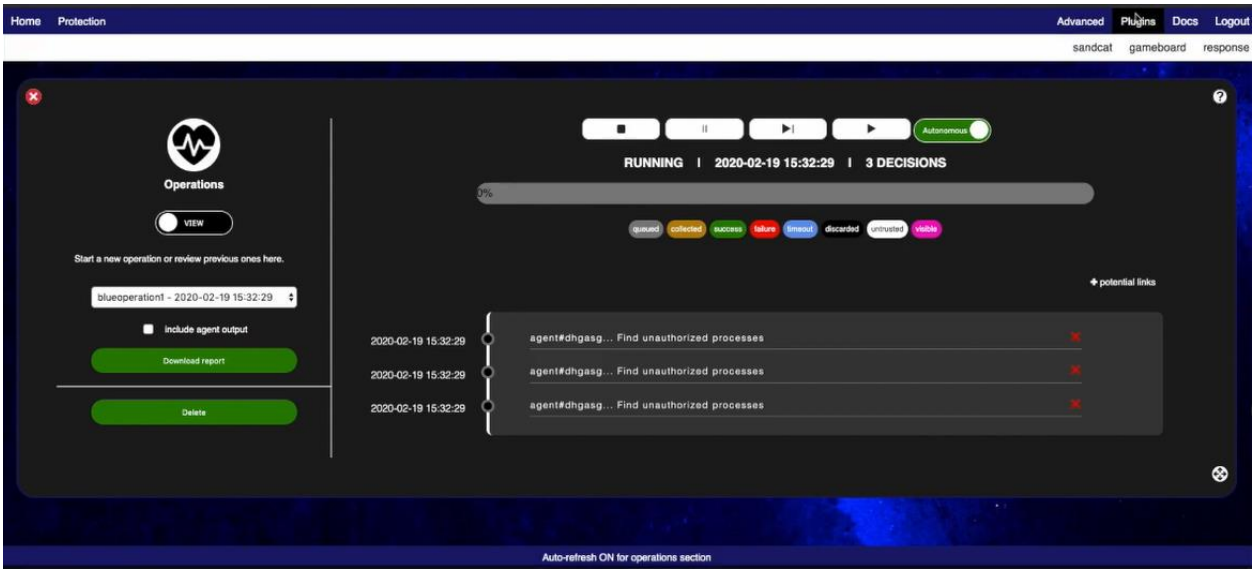
Automated Blue Teaming

Next Gen SOC teams can use MITRE ATT&CK framework as a security playbook. They can develop, test and deploy, automated incident response workflows based on the ATT&CK adversarial behavior. There are two way in which this can help.

1. Running this automated playbooks can detect any existing vulnerability and gives a comprehensive view of the existing security coverage. This helps in proactive detection and mitigation. Also identify gaps in the coverage which needs attention.
2. Next one is to automatically respond to the security incidents using the automated workflows, saving time, money and energy.

MITRE Caldera project is another software developed and maintained by MITRE Corporation. With Caldera, the Blue teams can emulate the incident response procedures to mitigate the ATT&CK Tactics and Techniques. The analysts can either run the procedures that are already prescribed in the ATT&CK Framework or develop custom procedures, create new tactics and techniques, procedures to detect and respond to the adversarial activities. Using Caldera APIs, one can create automated scrips, which can call the procedures or workflows in Caldera when there is an alert generated by SIEM tools. Caldera also allows to generate and download a comprehensive debrief document which contains details information about the operation performed, its behavior and the result.





Caldera also offers plugins where you can create fake agents on which the engineers can run their AI and ML algorithms and fine tune them for better detection.

Overall, Caldera helps in automated incident response and testing the security posture of the IT systems.

Conclusion

Reducing false positive, faster incident response and security content development and enrichment have been the focus areas of SOC teams. The ATT&CK Framework provides useful, relevant information and helps in identifying and filling the gaps in security coverage. So the features of the ATT&CK framework have a major impact on SOC team operations since it directly influences the working and efficiency of the SOC teams. The present day SOC may not be using ATT&CK framework very effectively, however the Next-Gen SOC will rely greatly on ATT&CK Framework from ideation phase to production. There is a great deal of contributions still needed to enhance and make the ATT&CK framework an ultimate knowledge base which security personal can use to develop a robust threat model.

The transition from Traditional SOC to SOC based on RBA is not easy and cannot be done as any other project with strict deadline. It is an organic process which consumes a lot of time and energy to evolve. But when it is done, the resulting cultural change will make the Security posture like never before. MITRE ATT&CK framework plays a major role in bring out such transition.

References

- https://www.exabeam.com/explainers/mitre-attck/what-is-mitre-attck-framework-and-how-your-soc-can-benefit/
- https://socradar.io/create-more-effective-soc-with-the-mitre-attck-framework/
- 10-ways-to-take-the-mitre-att-and-ck-framework-from-plan-to-action by Splunk
- https://www.splunk.com/en_us/blog/security/risk-based-alerting-the-new-frontier-for-siem.html
- https://lantern.splunk.com/Security/Product_Tips/Enterprise_Security/Implementing_risk-based_alerting
- https://www.guidepointsecurity.com/blog/taking-back-control-of-your-soc-with-risk-based-alerting/
- https://www.servicenow.com/products/security-operations.html
- https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/infographic/info-operationalizing-the-mitre-attack-framework.pdf
- https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/white-paper/security-operations-use-case-guide.pdf
- https://www.servicenow.com/products/vulnerability-response.html
- https://docs.servicenow.com/en-US/bundle/tokyo-it-service-management/page/product/change-management/concept/change-risk-assess-detect-conflict.html
- https://docs.servicenow.com/bundle/tokyo-it-service-management/page/script/server-scripting/reference/r_ChangeRiskCalculator.html
- https://github.com/center-for-threat-informed-defense/attack_to_cve
- https://dl.acm.org/doi/fullHtml/10.1145/3465481.3465758
- https://www.servicenow.com/lpwhp/soar-mitre-attack.html