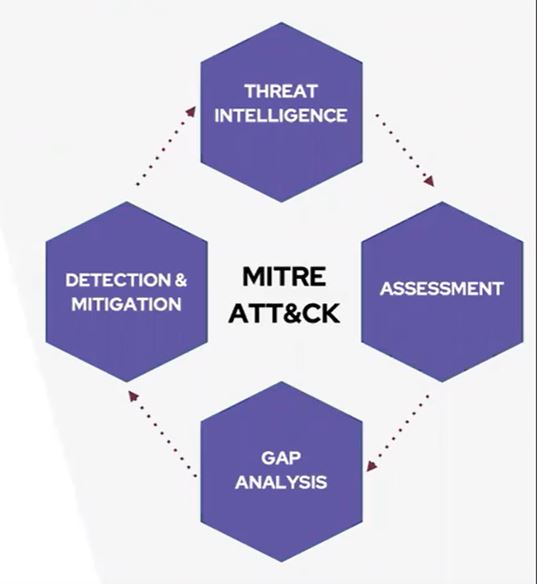
**Operationalize MITRE ATT&CK for Your SOC?**

**Implementing MITRE ATT&CK framework on SOC**



Simply MITRE Framework can be used for:

1. **Threat Intelligence:** Using ATT&CK as a threat intel source
2. **Assessment:** Using ATT&CK to access your defence
3. **Gap analysis:** Using ATT&CK to identify defensive gaps
4. **Detection and Mitigation:** Using ATT&CK to address the defensive gaps
5. **Threat Intelligence**

Understanding Attack helps us to understand the attacking behaviour of the adversary. Threat intelligence helps us by revealing the information of the adversary such as county / country origin. The sectors that adversary attack and so on. Also threat intelligence helps to understand the tactics, technique and behaviour of the adversaries with what tools and strategy they use. Threat intelligence also helps to understand the overall APT threat actors.

1. **Assessment**

In this process, several defence personnel are required in order to execute assessment. ATT&CK assessments are a part of a larger process to provide useful data to security engineers and architects justifying threat-based security improvements:

* Assess how your defences currently stack up to techniques and adversaries in ATT&CK,
* Identify the highest priority gaps in your current coverage, and
* Modify your defences — or acquire new ones — to address those gaps.

For assessment, Atomic Test can be used as Atomic Red Team can be used as library of simple tests that every security team can execute to test their defences. Tests are focused, have few dependencies, and are defined in a structured format that can be used by automation frameworks.

1. **Gap analysis**

ATT&CK can provide a valuable checklist of sorts for gap analysis in the SOC. It also provides a common terminology for threats across the organization and the numerous tools in the security infrastructure. Unless you have an unlimited security budget, it probably isn’t possible to try and cover every technique. Therefore, you need to prioritize carefully to minimize risk. That’s where D3 comes in. Mostly deals with logging gap and detection gaps. Logging gaps as you might not pull the right data source and detection gaps as you might not detect the technique gap.

**Detection and Mitigation**

The first step to creating and using ATT&CK analytics is understanding what data and search capabilities you have. In order to find suspicious behaviours, after all, you need to be able to see what’s happening on your systems. One way to do this is to look at the Data Sources listed for each ATT&CK technique. Those data sources describe the types of data that could give you visibility into the given technique. In other words, they give you a good starting point for what to collect. Process and process command line monitoring, often collected by Sysmon, Windows Event Logs, and many EDR platforms

File and registry monitoring, also often collected by Sysmon, Windows Event Logs, and many EDR platforms

Authentication logs, such as those collected from the domain controller via Windows Event Logs

Packet capture, especially east/west capture such as that collected between hosts and enclaves in your network by sensors such as Zeek

Once you know what data you have, you’ll need to collect that data into some kind of search platform (SIEM) so you can run analytics against it. You might already have this as part of your IT or security operations, or it might be something new you need to build. For these screenshots and the walkthrough, I’ll be using ELK (Elasticsearch/Logstash/Kibana) with Sysmon data, but there are a number of commercial and open source offerings and we don’t recommend any specific platform. Don’t underestimate these steps in the process, tuning your data collection is often the hardest part.