**A system to evaluate the implementation of**

**MITRE ATT&CK™ framework using a given set of logs**

**Shir Bar**

**Kfir Ram  
Hen Dahan**

**Introduction**

MITRE ATT&CK is an open framework and knowledge base of adversary tactics and techniques based on real-world observations. ATT&CK provides a common taxonomy of the tactical objectives of adversaries and their methods. Having a taxonomy by itself has many valuable uses, such as providing a common vocabulary for exchanging information with others in the security community. However, it also serves as a real technical framework for classifying organizations current detection efforts and identifying gaps where they are blind to certain types of attack behaviors. The main problem is that there is no tool today in the market that can evaluate the value of a source data set (logs) when being used with the MITRE ATT&CK for IT and ICS [1] for detecting cyber-attack techniques.

The proposed system will allow a method to denote what logs are being collected and from which systems. The logs will be correlated with the MITRE ATT&CK data and will output the list of ATT&CK techniques that can be identified using the logs. The system will allow the compilation of cyber security attacks based on threat intelligence and using ATT&CK IDs.  
The system enable organizations to assess their readiness for cyber- attacks.

In these days there is a tool called EVENTLIST developed by Miriam Wiesner, security program manager for Microsoft defender ATP.  
Miriam's software development was sponsored by Microsoft, System Frontier, Script Runner and Powershell.one.  
Although Microsoft is one of the sponsors Miriam's software is not supported by Microsoft, but by Miriam.  
The development process took quite a time and work, the EventList software is the closest software to the product we want to develop in our final project, it is a similar product but from the other direction.  
Miriam's EventList software receives as input one or several techniques we want to "locate" in the system and return as an output the logs with which you can detect the given techniques.  
unlike the software we will develop in this project, our software will receive as an input one log or several logs and will return as an output a list of techniques that can be detect by those logs.

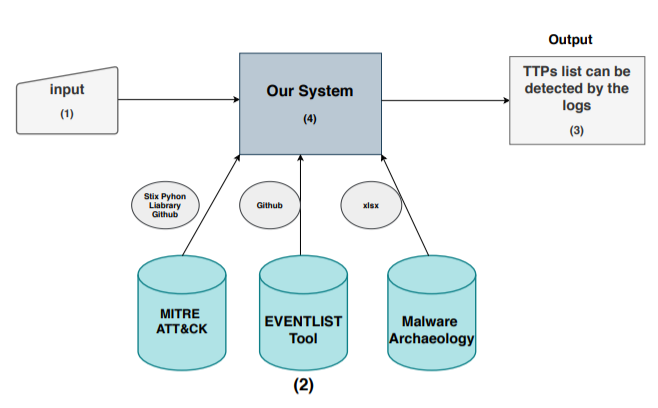


Figure 1

1. **Input –** The input of the system are the log files collected by the customer.   
   It is the customer's responsibility to collect the logs into an xml file.

It can be done easlly with EventViewer and Sysmon which are the tools that displays and collect the logs on computer.

**Logs ,high-level definietion:**In computing, a log file is a file that records either events that occur in an operating system or other software runs, or messages between different users of a communication software.Event logs record events taking place in the execution of a system in order to provide an audit trail that can be used to understand the activity of the system and to diagnose problems.

1. **Tools and databases-**In our system we will use 3 different tools and databases:

* **MITRE ATT&CK**- a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations of cyber security threats. They're displayed in matrices that are arranged by attack stages, from initial system access to data theft or machine control.

We will use MITRE ATT&CK in order to find TTPs after we will arange the input.

To ineract with MITRE ATT&CK API we need to use STIX python library.

* **Miriam Wiesner tool -** Miriam Wiesner, security program manager for Microsoft defender ATP.  
  Miriam's EventList software receives as input one or several techniques we want to "locate" in the system and return as an output the logs with which you can detect the given techniques.  
  Since our software will do the opposite action- receive as an input several logs and will return a list of techniques that can be detect by those logs as an output.
* **Malware Archaeology-** In looking into compromised systems, often what is needed by incident responders and investigators is not enabled or configured when it comes to logging. To help get system logs properly **Malware Archaeology** created some cheat sheets that help do logging well and so the.

One of the sheets they created , "The MITRE ATT&CK Logging Cheat Sheets" is very nesseccery for our work since this sheet present MITRE ATT&CK techniques classified to Microsoft and Sysmon event IDs.

1. **TTPs list can be detected by the given logs -** the final product of our software is a list of TTPs that can be detected by the given logs we get as an input.

This list will be an indication to customer about their readiness for cyber- attacks that consists of techniques and tactics.

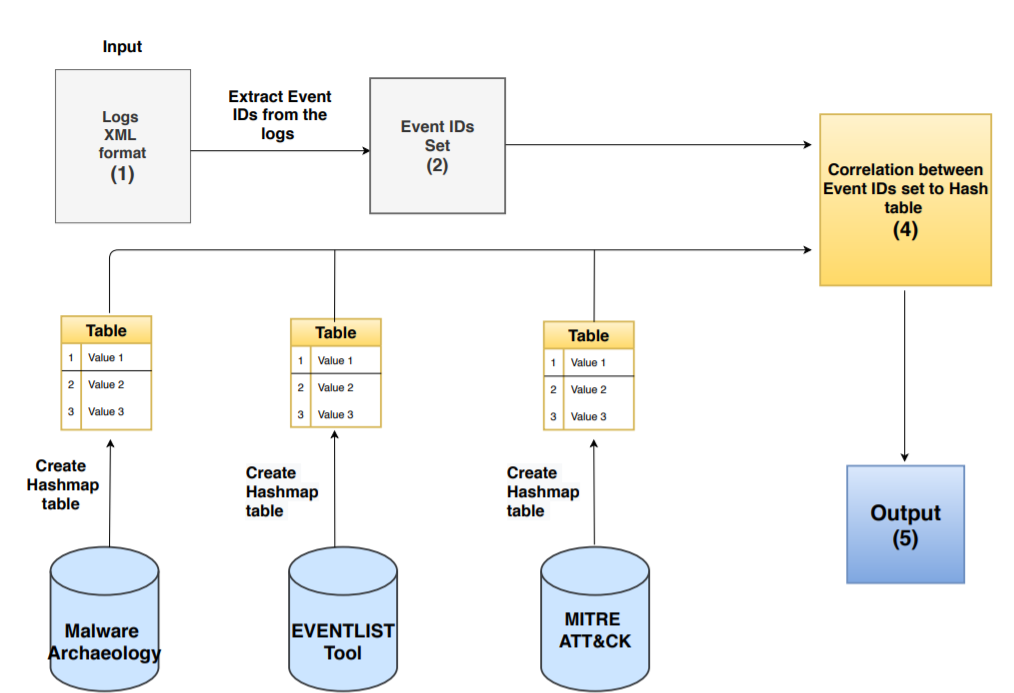
1. **Our System –** To understand better our system we will explain the following chart:

Figure **2**

**(3)**

**(1) Logs XML format**

**(2) Event IDs Set –** From the logs input which presents in XML format we will extract the Event ID in order to create Event IDs list that collected by the customer.   
To ensure that there are no repetitions of event IDs code in the list , we will use Set data structure.   
  
**(3) Create Hashmap tables-** As we mentioned before we will use 3 different databases as sources.   
Following to customer demande in the first menue the customer will be able to chosee which Data sources he want to use.

The customer will be able to choose one or more data sources.

For each data source that choosen we will create a hashmap table that consist of two columns:

* Key cell – the key will be the event ID
* Techniques – a set of thechinques related to the event ID.

Although it sounds like a simple task, it is not a simple task at all due to the structure of the data base we use.

1. **(4) Correlation between Event IDs set to Hashtable –** After we created hashtables we can performed the last task that lead us to the final reasult.

Since we have arrange hashtables of events IDs and thecniques, we can search in the table for each value (event id) in the set, the techniques that related to him.

We will store the set of reasults and print it on the screen.

**MITRE ATT&CK**

MITRE ATT&CK is an open framework and knowledge base of adversary tactics and techniques based on real-world observations.  
ATT&CK provides a common taxonomy of the tactical objectives of adversaries and their methods.

Using MITRE ATT&CK in Threat Detection with windows logs is one of our main goals in the project.

The article “*Using MITRE ATT&CK™ in Threat Hunting and Detection”* [2]   
present a several ways to make practical use of ATT&CK with a focus on threat hunting a detection.

Randy Franklin Smith, who is an internationally recognized expert on the security and control of Windows and AD security, along with Brian Coulson and Dan Kaiser, who works at LogRhythm Labs, present methods for detecting certain techniques with the help of logs and other tools. They present some basic tactics that most of the attacks are using, and some common techniques used by hackers.  
They are showing ways of how to find and how to deal with the repeated attacks.

In addition, the article presents five specific techniques from ATT&CK, which selected based on prevalence and other criteria that make them especially applicable to threat hunting and detection.   
The research explores each one of these techniques in-depth, highlighting how the attackers use them and how to detect them.

**Tactics, Techniques and Procedures (TTPs) Based Hunting Significance**

The main goal of the project is to enable organizations to assess their readiness for cyber-attacks.

To get this goal, we should use a method to detected malicious activity.  
There are many methods used to detected malicious activity.

Roman Daszczyszak et al. (2019) presents in their article [1] that many methods exist in these days and they also performed a comparison between the methods.

TTPs are representations of the behavior or modus operandi of cyber adversaries. It is a term taken from the traditional military sphere and is used to characterize what an adversary does and how they do it in increasing levels of detail.

The researchers are strongly convinced that collecting and filtering data based on knowledge of adversary tactics, techniques, and procedures (TTPs) is an effective method for detecting malicious activity.

Signature-based, anomaly-based, and TTP-based detection are complementary approaches to one another. However, the relative costs and effectiveness of each approach dictate a significant shift in how these approaches are employed. Because of its efficiency and relatively low investment, TTP-driven hunting may yield benefits far greater than the costs

Because of its efficiency and relatively low investment, TTP-driven hunting may yield benefits far greater than the costs.

In this article [2] the research describes the significance of TTP and mentioned that MITRE ATT&CK™ is the best frame that presents a categorized enumeration of those techniques.

Hunt analysts should determine data collection requirements to detect those techniques.  
System owners should deploy, activate, and/or configure sensors to continuously collect the data required to detect those techniques  
and Cyber platform developers should incorporate as much native sensing capability as possible into their systems to facilitate this approach (e.g., Microsoft Sysmon and Windows Event Logging).

**Retrieving ATT&CK Tactics and Techniques**

One of our main challenges is the ability of retrieving ATT&CK tactics and techniques from the logs.  
Every log file contains many activities; most of them are ordinary, our system will need to find a malicious set of logs and connect them to one of the many techniques exists in MITRE ATT&CK.

Threat intelligence sharing has been expanding during the last few years, leading cybersecurity professionals to have access to a large amount of opensource data.   
Among those, the tactics, techniques, and procedures (TTPs) related to a cyber threat are particularly valuable.

Therefore, the information provided by these means can either be structured (e.g. IP blacklists) or unstructured.

Whereas structured data can be accessed simply by using web scrapers or parsers, unstructured data require either manual analysis or natural language processing (NLP) tools, to extract the most relevant information.

We consider the logs to be unstructured data.

In this study [3], the research evaluates different multi-label text classification models to retrieve TTPs from textual sources, based on the ATT&CK framework, which is also the framework we will work with.

**Event Log Analysis**

An event is an observable activity that occurs on the system. The Windows event logging service can record five different types of event record: Error, Warning, Information, Success Audit, and Failure Audit. All of these have a defined set of data recorded for each event.  
Identifying malicious behavior from thousands of event log records of varying event ID types is not an easy challenge. Event logs provide a wealth of data to incident responders, but only if they are properly configured and retained.  
The event logging service can generate a vast amount of information about account logons, file and system access, changes to system configurations, process tracking, and much more.  
By understanding and using event logs efficiently, incident handlers can detect malicious actors, reconstruct a vast amount of adversary activity, and identify impacted systems.  
There is a connection between log event IDs to malicious attacks, for example, a series of failed 4776 events with Error Code C000006A (the password is invalid) followed by an Error Code C0000234 (the account is locked out) may be indicative of a failed password guessing attack.  
which is related to MITRE ATT&CK tactic ID TA0006 Credential Access and technique ID T1110 Brute Force number 001 Password Guessing.

Since our implementation of MITRE ATT&CK framework evaluation based on a given set of logs, we investigated on how to detect malicious actor's information in those set of logs.

This article [6] provides event IDs and specific indicators that can be used to detect and respond to malicious actors. Furthermore, it explains the advantages of aggregating these logs into a centralized location, which can help and make the process of searching through the logs easier.

**Communication of Standardized Cyber Threat Information, MITRE ATT&CK**

While cyber threat intelligence and information sharing can help focus and prioritize the use of the immense volumes of complex cyber security information organizations face today, they have a foundational need for standardized, structured representations of this information to make it tractable. The Structured Threat Information eXpression (STIX™) is a quickly evolving, collaborative community-driven effort to define and develop a language to represent structured threat information. The STIX language is meant to convey the full range of cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible.

Since we are working with MITRE ATT&CK framework, we investigate which structured language is the efficient for represent cyber threat information from MITRE ATT&CK.

The articles [4], [5] describes STIX advantages and explanations about how to work with this language using python.

STIX is a language, being developed in collaboration with all interested parties, for the specification, capture, characterization, and communication of standardized cyber threat information. It does so in a structured fashion to support more effective cyber threat management processes and application of automation.

A variety of high-level cyber security use cases rely on such information including:

* Analyzing cyber threats
* Specifying indicator patterns for cyber threat
* Managing cyber threat response activities
* Sharing cyber threat information

STIX provides a common mechanism for addressing structured cyber threat information across and among this full range of use cases improving consistency, efficiency, interoperability, and overall situational awareness.

In addition, STIX provides a unifying architecture tying together a diverse set of cyber threat information.

**Conclusion and Solution**

Knowledge of adversary tactics, techniques, and procedures (TTPs) is an effective method for detecting malicious activity and we will use what we learned in TTP based hunting [1] in order to detect malicious activity based on MITRE ATT&CK.

MITRE ATT&CK is a powerful way to classify and study adversary techniques and understand their intent. ATT&CK used in many ways to improve cybersecurity efforts based on [3].  
We will base our system on this framework to identify TTPs in the system logs.

The system will need to correlate with MITRE ATT&CK content and connect to MITRE ATT&CK Database.  
We decided to use STIX format to connect to MITRE ATT&CK database and correlate by utilizing cti-python-stix2 based on STIX articles [4], [5].

The system log file inserted to our system will include many events, our system will detect several logs depend on the first configuration we will filter based on common potential malicious logs shown in Event Log Analysis [6].

**Research questions:**

1. How can we automatically retrieve ATT&CK tactics and technique from specific logs?
2. Which tactics and techniques we should focus on our project? What are the common tactics and techniques that used in most of the attack?
3. How can we determine which logs are connected to a possible TTP?
4. How can we make the process of searching malicious movements through the logs faster?

**Research answers:**

1. MITRE ATT&CK main website (attack.mitre.org) has Detection section for each technique with detailed explanation of how to be able to detect a certain technique based on articles, with this information we will create a platform in our system to match logs to techniques.
2. We will focus on Windows techniques.
3. By using so many event IDs provided in article [6], which specify indicators that can detect malicious actors connected to a certain TTP.
4. We can make the process of searching malicious movement through the logs faster by normalizing the events of the logs, making a white list for ordinary events, and filtering out the potentially malicious logs.

**References:**

[1] Roman Daszczyszak, Dan Ellis, Steve Luke, Sean Whitley (March 2019).  
 TTP-Based Hunting

[2] LogRhythm (March 2019). Using MITRE ATT&CK™ in Threat Hunting and Detection.

[3] Valentine Solange Marine Legoy (November 2019). Retrieving ATT&CK tactics and techniques in cyber threat reports.

[4] Sean Barnum (February 20, 2014). Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)

[5] Structured Threat Information eXpression — STIX™

[6] Steve Anson (October 08, 2019). Event Log Analysis.