FINAL REPORT

Technology stack: AI for cyber security with IBM Qradar

Project Title: Advanced Techniques in Rule creation for Threats Detection.

Team ID: LTVIP2024TMID12665

Team no.: 1

Team Members: 1

1. MARPU KANVITH

COLLEGE: DR LANKAPALLI BULLAYYA COLLEGE VISHAKHAPATNAM

Index

INTRODUCTION

Cyber threat actors conduct malicious cyber threat activity by exploiting technical vulnerabilities, employing social engineering techniques, or by manipulating social media. A determined and capable adversary will often carefully select the technique most likely to result in successful exploitation after conducting reconnaissance against their target and may use a range of techniques to achieve their goal. The majority of threat actors, however, simply cast a wide net in hopes of exploiting any unsecure network or database.

Technical vulnerabilities are weaknesses or flaws in the design, implementation, operation, or management of an information technology system, device, or service that provides access to cyber threat actors. For example, a threat actor may attempt to install malicious software, called malware, or take advantage of existing flaws to exploit the targeted system. In addition to installing malware, threat actors also use tools that directly exploit specific technical vulnerabilities.

Exploitation methods that target human vulnerabilities, such as carelessness and trust, are collectively known as social engineering. Threat actors use social engineering to trick an individual into inadvertently allowing access to a system, network, or device. Phishing and spear-phishing are common social engineering techniques. (Please see Annex A: The cyber threat toolbox for more information).

Cyber threat actors can also manipulate social media in order to influence public discourse. With a thorough understanding of how traditional media and social

media work – and how individuals consume information – cyber threat actors can promote their message to broader target audiences at a relatively low cost. They can do this by masquerading as legitimate information providers, hijacking social media accounts, or creating websites and new accounts.

Attribution is the act of accurately determining the threat actor responsible for a particular set of activities. Successful attribution of a cyber threat actor is important for a number of reasons, including network defence, law enforcement, deterrence, and foreign relations. Cyber threat actors attempt to evade attribution through obfuscation.

Obfuscation refers to the tools and techniques that threat actors use to hide their identities, goals, techniques, and even their victims. In order to avoid leaving clues that defenders could use to attribute the activity, threat actors can use either common, readily available tools and techniques or custom-built tools that covertly send information over the Internet.

Sophisticated threat actors can also use false flags, whereby an actor mimics the known activities of other actors with the hope of causing defenders to falsely attribute the activity to someone else. For example, a nation-state could use a tool believed to be used extensively by cybercriminals.

The ability of cyber threat actors to successfully obfuscate their actions varies according to their level of sophistication and motivation. In general, more sophisticated actors, such as nation-states and competent cybercriminals, will be more adept at – and have more reasons for – obfuscation and will be more

ABSTRACT

Cyber incidents that target ICSs are security, safety, and business problems. Such abnormal events affect physical devices, such as actuators and sensors. If a cyberattack results in manufacturing operations being shut down, a company will lose significant revenue. In addition, if a cyberattack targets systems that require safety operations, the operators will be endangered. For example, cyberattacks on an iron furnace have been reported [2]. In addition to safety risks, cyberattacks continue to pose serious financial risk for companies [3]. Therefore, cyberattacks should be prevented to ensure corporate resilience.

In addition to awareness of potential cyberattacks, the need for cybersecurity training has increased. The National Institute of Standards and Technology (NIST) specifies that incident response teams should be assigned and trained to develop incident response capabilities against cyberattacks. NIST SP 800-61 [4] describes the ability required for an incident response as follows: "Managers should be technically adept and have excellent communication skills." A capability for an incident response requires technical skill and non-technical skill. Several authorities have developed tabletop cybersecurity exercises to improve technical security awareness. Tomomi et al. described a technical exercise from

perspective of non-technical skills [5]. However, most security exercises focus onthe technical aspects of incident responses. In other words, they are not designed to evaluate a team's non-technical skills even though it is obvious that team'snon-technical skills will affect overall performance.

Stage -1

Title of the Project : Advanced Techniques in Rule creation for Threats

Cyber threat actors are not equal in terms of capability and sophistication, and have a range of resources, training, and support for their activities. Cyber threat actors may operate on their own or as part of a larger organization (i.e., a nation-state intelligence program or organized crime group). Sometimes, even sophisticated actors use less sophisticated and readily available tools and techniques because these can still be effective for a given task and/ or make it difficult for defenders to attribute the activity.

Nation-states are frequently the most sophisticated threat actors, with dedicated resources and personnel, and extensive planning and coordination.

Cybercriminals are generally understood to have moderate sophistication in comparison to nation-states. Nonetheless, they still have planning and support functions in addition to specialized technical capabilities that affect a large number of victims.

Threat actors in the top tier of sophistication and skill,

capable of using advanced techniques to conduct complex and protracted campaigns in the pursuit of their strategic goals, are often called advanced persistent threats (APT). This designator is usually reserved for nation-states or very proficient organized crime groups.

Hacktivists, terrorist groups, and thrill-seekers are typically at the lowest level of sophistication as they often rely on widely available tools that require little technical skill to deploy. Their actions, more often than not, have no lasting effect on their targets beyond reputation.

Insider threats are individuals working within their organization who are particularly dangerous because of their access to internal networks that are protected by security perimeters. Access is a key component for malicious threat actors and having privileged acess eliminates the need to employ other remote means. Insider threats may be associated with any of the other listed types of threat actors

The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by RiskBased Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

Medical services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

With the scale of the cyber threat set to continue to rise, global spending on cybersecurity solutions is naturally increasing. Gartner predicts cybersecurity spending will reach $188.3 billion in 2023 and surpass $260 billion globally by 2026. Governments across the globe

have responded to the rising cyber threat with guidance to help organizations implement effective cyber-security practices.

In the U.S., the National Institute of Standards and Technology (NIST) has created a cyber-security framework. To combat the proliferation of malicious code and aid in early detection, the framework recommends continuous, real-time monitoring of all electronic resources.

The importance of system monitoring is echoed in the "10 steps to cyber security", guidance provided by the U.K. government's National Cyber Security Centre. In Australia, The Australian Cyber Security Centre (ACSC) regularly publishes guidance on how organizations can counter the latest cyber-security threats.

Stage -2

(detection of threats and types of threats)

Description:

Types of threats :

In the simplest sense, a cybersecurity threat, or cyberthreat, is an indication that a hacker or malicious actor is attempting to gain unauthorized access to a network for the purpose of launching a cyberattack.

Cyberthreats can range from the obvious, such as an email from a foreign potentate offering a small fortune if you'll just provide your bank account number, to the deviously stealthy, such as a line of malicious code that sneaks past cyberdefenses and lives on the network for months or years before triggering a costly data breach. The more security teams and employees know about the different types of cybersecurity threats, the more effectively they can prevent, prepare for, and respond to cyberattacks

Malware

Malware—short for "malicious software"—is software code written intentionally to harm a computer system or its users.

Almost every modern cyberattack involves some type of malware. Threat actors use malware attacks to gain unauthorized access and render infected systems inoperable, destroying data, stealing sensitive information, and even wiping files critical to the operating system.

Common types of malware include

Ransomware:: locks a victim's data or device and threatens to keep it locked, or leak it publicly, unless the victim pays a ransom to the attacker. According to the IBM Security X-Force Threat Intelligence Index 2023, ransomware attacks represented 17 percent of all cyberattacks in 2022.

A Trojan horse : is malicious code that tricks people into downloading it by appearing to be a useful program or hiding within legitimate software. Examples include remote access Trojans (RATs), which create a secret backdoor on the victim's device, or dropper Trojans, which install additional malware once they gain a foothold on the target system or network.

Spyware :: is a highly secretive malware that gathers sensitive information, like usernames, passwords, credit card numbers and other personal data, and transmits it back to the attacker without the victim knowing.

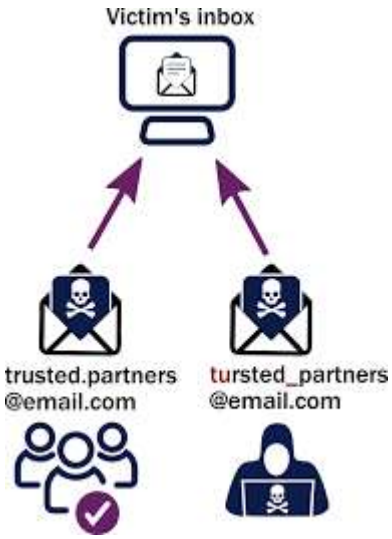
Worms are self-replicating programs that automatically spread to apps and devices without human interaction.

Common types of phishing include:

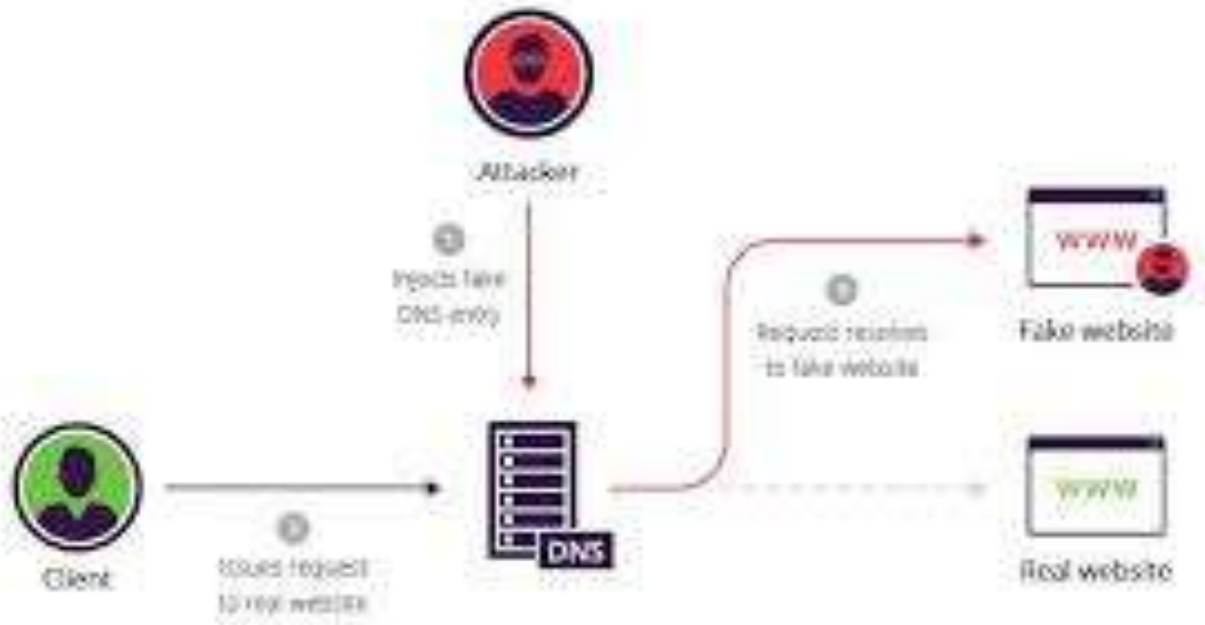
Spear phishing—highly targeted phishing attacks that manipulate a specific individual, often using details from the victim's public social media profiles to make the scam more convincing.

Whale phishing—spear phishing that targets corporate executives or wealthy individuals.

Business email compromise (BEC)—scams in which cybercriminals pose as executives, vendors, or trusted business associates to trick victims into wiring money or sharing sensitive data.



Another common social engineering scam is domain name spoofing (also called DNS spoofing), in which cybercriminals use a fake website or domain name that impersonates a real one—e.g., 'applesupport.com' for support.apple.com—to trick people into entering sensitive information. Phishing emails often use spoofed sender domain names to make the email seem more credible and legitimate



Stage 3 (tools in of the threat in cyber security) :

. TOOLS USED IN CYBERSECURITY

A. aswMBR

aswMBR is a anti-rootkit scanner that searchs your computer for Rootkits that infect the Master Boot Record, or MBR, of your

computer. This includes the TDL4/3, MBRoot (Sinowal), and Whistler rootkits. For this program to properly work it must first

download the Avast virus definitions, so you will need an active Internet connection before using it. A rootkit is

a malware program that is designed to hide itself or other computer infections on your computer. These types of programs are

typically harder to remove than generic malware, which is the reason that stand-alone utilities such as TDSSKiller have been

developed. When you run aswMBR, if it is shutdown automatically, then it is most likely the infection detecting that aswMBR is

running and terminating it. In this situation you should rename executable to iexplore.exe before you attempt to run it.

aswMBR is a utility program designed to work in conjunction with other antivirus software to keep your computer safe from

malware and other unwanted programs. It can complete thorough scans for rootkits associated with malware programs and

remove them when a conventional uninstaller or antivirus cannot.

ADVANTAGES aswMBR

1. Quick and efficient: This program scans and performs repairs quickly. There are no fancy features involved, but you also don't

have to tie up your computer for long periods of time to rid it of unwanted programs.

2. Avast antivirus compatibility: While aswMBR is not a complete antivirus program, it is made to work with Avast Free

Antivirus, which you have to download and install separately. Together, they comprise a complete solution to your system

protection needs.

3. Not for beginners: This program does not come with a Help feature, and the interface is as utilitarian as they come. If you don't

already know your way around this type of tool or know how to interpret the scan results, this program won't be of much use to

you. If you have some advanced computer knowledge and want to make sure your machine is free from all elements of malware

programs, this is a good choice. It's free, and it does exactly what it promises. But it was not designed to be a one-stop solution

for your antivirus needs. It's also not terribly accessible

B. CATCHME

Catchme is a powerful utility designed by gmer.net to remove malware and other malicious files.It is NOT an antivirus program – it IS a virus removal tool..

It does not have a bloated user interface and quickly and efficiently cleans your system.

Unlike a mainstream antivirus program such as Symantec, kaspersky or McAfee, it is free and you do not install it and it will not slow your system to a halt. Simply download it , run it click scan button and allow catchme to scan your system.

The file, catchme.exe, that can be downloaded below is hosted right here on proposedsolution.com, a trusted source.

 Catchme.exe removes thousands of known viruses such as trojans and worms.

 Works for all current versions of Windows up to Vista (try later versions, it might work).

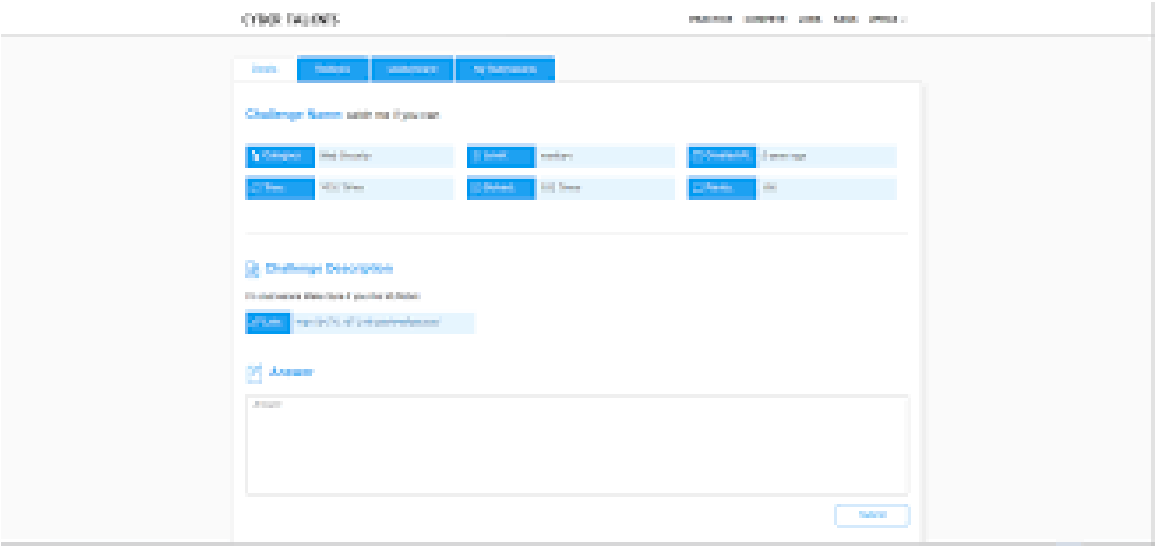
 You need administrator access for this to work (default for most Windows users).

Usage Instructions

To download catchme please do the following:

1. Click the ‘Like‘button in the download area below to reveal the download links .
2. Save the file catchme.exe to your desktop.
3. Double-click catchme.exe and it will extract launch a simple user interface.
4. Click the scan button. A dos window will launch and display progress messages.

5. When the scan is finished, go to the Scripts tab and click the Run button if anything was found.
6. Click Restart button. This download is provided free and without any guarantee that it will solve your problems.



C. GMER

Ease of Use GMER is a software tool for detecting and removing root kits. Written by a Polish researcher Przemysław Gmerek. It runs on Microsoft Windows and has support for Windows NT, 2000, XP, Vista, 7 and 8. With version 2.0.18327 full support for Windows x64 is added. A rootkit is a malware program that is designed to hide itself or other computer infections on your computer. These types of programs are typically harder to remove than generic malware, which is the reason that stand-alone utilities such as TDSSKiller have been developed. At the time of first release in 2004 it introduced innovative rootkit detection techniques and quickly gained popularity for its effectiveness. It was incorporated into a few antivirus tools including avast

antivirus and SDFix. For several months in 2006 and 2007, the tool's website was the target of heavy DDoS attacks attempting to block its downloads..

GMER is available as a random named .EXE files or a .ZIP file. When you run GMER, if it is shutdown automatically, then it is most likely the infection detecting that GMER is running and terminating it. In this situation you should use the .EXE download link to download a random named version of GMER. If you are unable to run that, then please rename the download to iexplore.exe before you attempt to run it.

GMER scans for the following:

- Hidden processes
- Hidden threads
- Hidden modules
- Hidden services
- Hidden files
- Hidden disk sectors (MBR)
- Hidden Alternate Data Streams
- Hidden registry keys
- Drivers hooking SSDT
- Drivers hooking IDT

SanityCheck:

SanityCheck is an advanced rootkit and malware detection tool for Windows which thoroughly scans the system for threats and irregularities which indicate malware or rootkit behavior. By making use of special deep inventory techniques, this program detects hidden and spoofed processes, hidden threads, hidden drivers and a large number of hooks and hacks which are typically the work of rootkits and malware. It offers a comprehensible report which gives a detailed explanation of any irregularities found and offers suggestions on how to solve or further investigate any situation.

SanityCheck Features

1. Runs on almost all Windows versions:SanityCheck runs on most recent Windows versions including Windows 7, Windows8, Windows Vista and Windows XP. For an exact overview of the Windows versions supported by SanityCheck and the service packs required.

2. Makes use of special deep inventory techniques:- SanityCheck makes use of a special Windows feature (a Global Flag setting) which allows it to create a deep inventory of drivers, devices, processes, threads and a lot of other information about yoursystem.

By making use of this feature in combination with other techniques it is able to create a very thorough scan of irregularities on your system.

3. Detect hidden processes: SanityCheck goes to incredible lengths to detect processes which hide themselves from the Windows

taskmanager and programming interfaces. It uses seven unmentioned safe techniques to reveal hidden processes in both usermode and kernelmode.

4. Detect obfuscated processes: Sanity Check detects processes which do efforts to obfuscate their names. This is a typical activity associated with malware.

5. Detect processes attempting to appear as common system processes :Sanity Check detects for processes which appear as as process.

6. Detect processes with obviously deceptive names: Malicious processes which are received as email attachements often try to appear as an innocent document types. An example of such a process name is:”foo.txt.exe”

7. Detect processes without product, company or description information: Although not necessarily evil, SanityCheck checks for

processes without a product, company or description resource information.

8. Verify signatures and checksums of processes and kernel modules: Sanitycheck verifies digital signatures on processes and kernel modules and checks them for validity. It also verifies the validity of checksums.

9. Detect SSDT hooks: SanityCheck detects kernel modules which hook the system service descriptor table. Although not necessarily the work of malware, SanityCheck will do every effort to detect the modules responsbile for these acts and generate a comprehensible report.

10. Detect Import Address Table hooks: The program detects kernel modules which hook the entry points of exported kernel routines.

11. Detect kernel object callout hooks :Although rarely used, kernel object callout hooks are incredibly powerful and have the potential to instrument the complete working of the Windows kernel. Currently we do not know of any security product which detects these hooks.

12. Detect hidden drivers :SanityCheck detects various forms of kernel modules which are attempting to hide.

13. Detect hijacked driver entry points :Hijacked dispatch entry points in drivers can be used by rootkits and malware for a wide variety of purposes. SanityCheck detects both drivers which have their entry points hooked as well as the modules reponsible for these actions.

14. Find the culprit :Note that it is not always possible to make a clear distinction between malware and legitimate products. This is because certain products resort to aggressive controversial techniques as anti-piracy measures, to avoid debugging or even for anti-competitive purposes. Anitivirus or other security software that is installed on your system may be making use of rootkit-like techniques such as a hidden process in an effort to hide itself from malware. Such products may be involved in a controversial race along the lines of "defeat evil with its own weapons". For this reason SanityCheck does everything possible to pinpoint the modules and processes which are responsbile for these actions while remaining careful in drawing any conclusions.

15. Comprehensible report :We do not believe in aggressively "fixing" malware with a single click of a button. This is because there is no such thing as a clear distinction line between malware and legitimate products which make of controversial techniques. "Fixing" hooks in the kernel is a very unsafe and despicable act which is only very likely to make your system crash or worse.
Instead Sanitycheck leaves your system in an unaltered state while offering comprehensible suggestions on how to proceed in any situation.

16. Optional expert mode: Optionally you can switch SanityCheck into expert mode. It will then display a wealth of information on drivers, devices, processes, threads, kernel objects and system routines which can be very useful for further analysis. A lot of

the information available in expert mode cannot be obtained by any other existing utility other than a kernel debugger. Because the amount of information can be overwhelming and may be difficult to understand for novice users, it is turned off by default and only a comprehensible report is displayed.

Report :

: Advanced Techniques in Rule creation for Threats Detection

Threat detection and response (TDR) is the process of identifying potential threats and reacting to them before they impact the business. TDR enables organizations to maintain a strong security posture to avoid security incidents, such as data breaches and data loss.

Effective threat detection and response is an increasingly difficult and ever-evolving challenge for security operations center (SOC)

teams. Previously, prevention technologies, including antimalware and antivirus software paired with a firewall, were sufficient to defend against cyber attacks. Today, organizations require a defense-in-depth security strategy that incorporates these technologies and more advanced TDR tools and processes to defend against the growing number and sophistication of cyberthreats. Increasingly dispersed workloads and cloud adoption have led to a growing attack surface, which has extended the challenge. Further, many security teams use either manual processes that don't scale in modern environments or disparate TDR tools that don't integrate properly, causing alert overload and fatigue for team members.

Conclusion :

Organizations and people alike face a continuous struggle as a result of the constantly shifting
terrain of cyber threats. Despite the fact that traditional methods of cybersecurity are necessary,
they are becoming increasingly insufficient in the face of threats that are rapidly being
developed. The purpose of this study was to investigate the valuable contribution that machine
learning may make to the enhancement of cybersecurity efforts, with a particular emphasis on

threat detection, prevention, and response. Throughout the course of this voyage, we have
investigated the various applications of machine learning. These applications include anomaly
detection and signature-based detection, as well as behavioural analysis, predictive analytics,
and natural language processing. A remarkable level of precision, speed, and adaptability has
been proven by these applications in their capacity to identify and combat threats.

Future scope :

Organizations and people alike face a continuous struggle as a result of the constantly shifting
terrain of cyber threats. Despite the fact that traditional methods of cybersecurity are necessary,
they are becoming increasingly insufficient in the face of threats that are rapidly being
developed. The purpose of this study was to investigate the valuable contribution that machine
learning may make to the enhancement of cybersecurity efforts, with a particular emphasis on
threat detection, prevention, and response. Throughout the course of this voyage, we have
investigated the various applications of machine learning. These applications include anomaly

detection and signature-based detection, as well as behavioural analysis, predictive analytics,
and natural language processing. A remarkable level of precision, speed, and adaptability has
been proven by these applications in their capacity to identify and combat threats.

References :

https://www.ibm.com/products/qradar-siem/advanced-threat-detection?utm_content=SRCWW&p1=Search&p4=43700078400677276&p5=p&gad_source=1&gclid=EAIaIQobChMIiJu5473uhQMV4Mk8Ah3mjAf1EAMYASAAEgIAmvD_BwE&gclsrc=aw.ds

https://www.snowflake.com/guides/threat-detection-methods

https://www.simspace.com/blog/threat-detection-and-response-best-practices-and-tips-for-success

https://datasciencedojo.com/blog/ai-in-cybersecurity/