Scientific Research Publishing

Engineering, 2023, 15, 798-809
https://www.scirp.org/journal/eng
ISSN Online: 1947-394X
ISSN Print: 1947-3931

Study on the Use of Artificial Intelligence for Cybersecurity in Companies: Case of Companies in Burkina Faso

Yanogo Kiswendsida Jean Hermann, Ouedraogo Tounwendyam Frederic

Institute of Computer Engineering, Telecommunication Polytechnic School of Ouagadougou, Ouagadougou, Burkina Faso
Email: yanogohermann@yahoo.fr

How to cite this paper: Hermann, Y.K.J. and Frederic, O.T. (2023) Study on the Use of Artificial Intelligence for Cybersecurity in Companies: Case of Companies in Burkina Faso. *Engineering*, **15**, 798-809.
https://doi.org/10.4236/eng.2023.1512056

Received: October 5, 2023
Accepted: December 8, 2023
Published: December 11, 2023

Abstract

Poorly secured connected objects can compromise the security of an entire company, or even paralyze others. As useful as they are, they can be open doors for computer attacks against the company. To protect themselves, large companies set up expensive infrastructures to analyze the data that circulates inside and outside the company. They install a SOC, a Security Operation Center whose objective is to identify and analyze, using various tools, the level of protection of a company and, if necessary, to alert on vulnerabilities and leaks of security data. However, the attack detection capabilities of traditional systems are based on a base of known signatures. Problem is that it is increasingly rare to have to face threats whose signature is unknown. Artificial intelligence, on the contrary, does not look for fingerprints in the packets carrying the attack, but rather analyzes how these packets are arranged. The objective of this study is to show that the use of artificial intelligence in companies may be low and to show the positive impacts of its use compared to the traditional system used in companies. We also simulate an attack on a system equipped with artificial intelligence to highlight the advantages of AI in a computer attack. This research is important because it highlights the risks that companies expose themselves to by always remaining secure in their systems based on traditional techniques. The aim of this research is to show the advantages that AI offers on cyber security compared to the traditional security system. The expected result is to show the existing issues regarding the rate of use of AI on cybersecurity in Burkina Faso.

Keywords

Cybersecurity, Artificial Intelligence, Computer System, Computer Attack, Information Security

1. Introduction

Tasks in companies are automated, resources assigned to users are centralized. New professions and new functions are appearing in the business world in order to optimize all daily tasks as well as the resources made available to users. In view of this rapid development of new technologies, flaws and vulnerabilities are exposed and exploited by a certain number of actors in order to harm businesses. These are, among other things, techniques used by those we call “Hackers”. This present phenomenon has developed over the years. To counter this growing phenomenon, new players have emerged in the IT professions. This is cybersecurity as a whole, consisting of computer security, cyberdefense and cybercrime. The current trend in the IT field is artificial intelligence. AI put at the service of cybersecurity, it allows computer systems through machine learning and deep learning to be more effective in detecting intrusions in a network and to fight effectively against them by providing adequate responses. It is important to say that artificial intelligence methods enable achieving much better results than traditional statistical methods [1]. The contribution of this research is to show the risks incurred by companies by relying on traditional systems (SOC, firewalls, etc.) to secure themselves instead of integrating artificial intelligence.

The IA is capable enough to bring intelligent decisions by interacting closely with a human being or autonomously [2].

2. Research Methodology Used

To carry out this research, we used the mixed approach which is both quantitative and qualitative. We also carry out an attack simulation in a computer system equipped with AI in order to analyze the result and compare to the traditional security system.

2.1. Research Techniques

In this research the following techniques are used.

2.1.1. The Interview Technique

During the interview, we ask a set of questions to the people responsible for managing the security system of each company. The answers to these questions are listed. Then we proceed to the analysis phase which consists of analyzing posture, availability, the way of responding as well as the responses obtained. We apply the validity test, the consistency test, and the distribution test on the answers obtained through our questions.

2.1.2. Documentary Technique

This involves gathering basic information. Then, we determine the types of document needed, whether articles, newspapers, magazines. Then we search for the corresponding references and in order we present the bibliography.

2.1.3. Sampling Technique

This involves selecting a subset of units from our target population in order to collect information. This information is used to draw conclusions about our general population. In other words we will select a few companies from a multitude.

2.2. Investigation Plan

The survey on the use of AI in the service of cyber security aims to collect, from IT security professionals, the mechanisms used to protect their IT system, and compare the risks they face compared to the use of AI.

2.3. Determination of Study Sample Size

Sampling is the operation which consists of taking a certain number of elements to process or observe, that is to say that the sample is a subset of the population. For our case, we use the formula which allows us to determine the sample size using 10% margin of error. We then apply:

$$N = Z^2 \,\&*P*Q/e^2$$

& = 0.5 implies that $Z = 1.96$

$P = 0.5$

$Q = 1 - p = 0.5$

$E =$ between 1% and 10%

N: represents the sample size

Z^2 = reduced center normal law

$\&$ = represents the degree of confidence

E^2 = represents the maximum or systematic error

We will therefore have

$$N = 1.962 \times 0.5 \times 0.5/0.12 = 0.2401/0.01 = 97$$

We will also simulate a computer attack on a system equipped with AI in order to better understand the advantages of AI.

3. The Advantages of AI Compared to the Traditional Security System

The first is that the attack detection capabilities of traditional systems rely on a base of known signatures. Problem is that it is increasingly rare to have to face threats whose signature is unknown. Artificial intelligence, on the contrary, does not look for fingerprints in the packets that carry the attack, rather it analyzes how these packets are arranged and, in this case, the patterns do not evolve. For the cyber attackers, it is always a question of accessing something specific such as a database, for example, with determined progress points.

The second problem, which follows from the previous one, is that traditional systems must analyze an ever-increasing number of signatures. They are therefore likely to degrade the performance of the IS to be protected. An open source database from a security publisher may offer to compare each incoming packet to more than 50,000 signatures, while a solution based on artificial intelligence may have no more than fifty typical behaviors to identify.

The third problem, finally, is that cyberattacks succeed in the vast majority of cases, not thanks to malware that a firewall could have stopped, but because the cyber-attacker bypassed the firewall. He deceived a user's vigilance with phishing. Once infiltrated on the network, the hacker now uses completely legitimate tools. These are typically those in targeted systems, which do not trigger any alarms, but are nevertheless used to obtain privileges. Here, traditional protection devices are powerless because they have nothing to evaluate. Artificial intelligence, on the other hand, will detect the attack because it observes the use of user accounts. The convergence of Artificial Intelligence (AI) and the cybersecurity has revolutionized various industries, including finance and technology (fintech). In the fintech sector, the integration of AI with cybersecurity has led to significant improvements in application security [3].

3.1. The Advantages of AI for Cybersecurity

As we explore the possible implications with security in machine learning and AI, it is important to frame the current challenges inherent in cybersecurity. There are many processes and aspects that we have long considered normal, which can be addressed under the umbrella of AI technologies.

3.1.1. Human Error in Configuration

Human error accounts for a large portion of cybersecurity weaknesses. For example, proper system configuration can be incredibly difficult to manage, even with large IT teams involved. In the race for constant innovation, IT security has become more hierarchical than ever. The right tools can help teams identify and mitigate issues that arise when network systems are replaced, modified, and updated.

The latest internet infrastructures like cloud computing can take over old local structures. The IT department must ensure the compatibility of business systems to protect them. Manual configuration security assessment processes exhaust teams as they juggle endless updates and mundane daily support tasks. With intelligent, adaptive automation, teams can benefit from timely advice on the latest issues detected. They can take advice on treatment options, or even have systems to automatically adjust parameters if necessary.

3.1.2. Human Efficiency and Recurring Tasks

Human efficiency is another challenge inherent to the cybersecurity industry. No manual process is perfectly repeatable every time, especially in dynamic environments like ours. Individually configuring a company's numerous terminals is one of the most time-consuming tasks. Even after initial configuration, IT may need to recheck the same machines later to correct inappropriate or outdated configurations that cannot be corrected through remote updates. What's more, when employees must respond to threats, the scope of those threats can quickly evolve. When human interventions can be slowed by unexpected challenges, an AI and machine learning-based system can operate with minimal delay.

3.1.3. Threat Alert Fatigue

Threat alert fatigue is another weakness if not carefully managed. Attack surfaces are expanding as the aforementioned security layers become more sophisticated and sprawling. Many security systems are configured to respond to a multitude of known problems, with a host of purely mechanical alerts. As a result, these individual prompts let IT analyze potential decisions and take appropriate action. A high flow of alerts significantly complicates decision-making. Ultimately, decision fatigue becomes a daily experience for cybersecurity personnel. The ideal solution lies in proactive actions against identified threats and vulnerabilities, but many teams lack both the time and personnel to cover all of their bases. Sometimes teams are forced to prioritize the most serious problems and let others fall by the wayside. Harnessing AI in cybersecurity can enable IT departments to manage more threats efficiently and conveniently. Automated labeling can significantly simplify the management of each of these threats. Additionally, some problems can be solved by the Machine Learning algorithm itself.

3.1.4. Response Time in the Event of a Threat

Response time in the event of a threat is one of the key factors in the effectiveness of a cybersecurity team. From exploitation to deployment, malicious attacks are known to progress extremely quickly. In the past, cybercriminals sometimes took weeks to breach network permissions and invalidate security measures before they could launch their attack. Unfortunately, experts in the cyber defense space are not the only ones who benefit from technological innovations. Automation is more common in cyberattacks today. Threats like attacks via the latest LockBit ransomware have significantly accelerated timelines. Today, half an hour is enough to launch certain attacks. The human response may lag behind the initial attack, even if it is known. It is for this reason that many teams are more inclined to react to actual attacks rather than preventing attempted attacks. On the other hand, undetected attacks pose a danger on their own. ML-driven security can extract data from an attack, aggregate it, and immediately prepare it for analysis. It can provide cybersecurity teams with simplified reports that will facilitate processing and decision-making. Beyond reporting, this type of security also provides recommended action that limits consequences and prevents future attacks.

3.1.5. Identification and Anticipation of New Threats

Identifying and anticipating new threats is another factor impacting response times in the event of a cyberattack. As stated previously, responses are already late with existing attacks. Unknown attack types, behaviors, and tools can also mislead a team and slow down the process. Worse, more discreet threats like data theft can sometimes go unnoticed. Cyberattacks are rarely designed from scratch. Because attacks are often developed from behaviors, structures, and source code from previous attacks, machine learning has a pre-existing path to build on.

Machine learning programming can help highlight commonalities between the new threat and previously identified threats to detect an attack. No team can complete this task quickly. This highlights the indispensable side of adaptive security models. From this point of view, Machine Learning can simplify the anticipation of new threats. It is important to declare that cyber threats are becoming more sophisticated and automation, make the protections ineffective. Conventional cybersecurity approaches have a limited effect on fighting new cyber threats. Therefore, we need new approaches, and artificial intelligence can aid to counter cybercrime [4].

4. Presentation, Analysis and Interpretation of Results

After collecting our data, we do the analysis on SPSS software and we obtain the following results: (**Table 1**)

Statistics

Do you use AI within your structure?

N	Valid	97
	Missing	0

We find that 92.8 percent do not use AI within their company. We have only 7.2 percent using AI as part of their cybersecurity.

However, artificial intelligence is an asset for improving cybersecurity in several ways. It can help detect threats by analyzing data and behavior to identify anomalies that could indicate an attack in progress. AI can also help automate security incident response by quickly identifying threat sources and taking action to contain them. Additionally, AI can be used to strengthen data protection by encrypting sensitive information and classifying it according to its confidentiality level. Finally, AI can help businesses protect against future attacks by analyzing threat data to determine trends and patterns of attacker behavior

Figure 1 shows us the proportions of AI use. We note that its use is low despite the advantages of AI. Indeed, AI technologies, such as deep learning, can be introduced into cyber security to construct smart models for implementing malware classification and intrusion detection and threatening intelligence sensing [5] (**Table 2**).

Statistics

Do you find it important to use AI within your business?

N	Valid	97
	Missing	0

Table 1. Rate of use of AI for cybersecurity.

Do you use AI within your structure?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oui	7	7.2	7.2	7.2
	Non	90	92.8	92.8	100.0
	Total	97	100.0	100.0	

Table 2. Opinions on the use of AI in business.

Do you find it important to use AI within your business?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Oui	94	96.9	96.9	96.9
	Non	3	3.1	3.1	100.0
	Total	97	100.0	100.0	

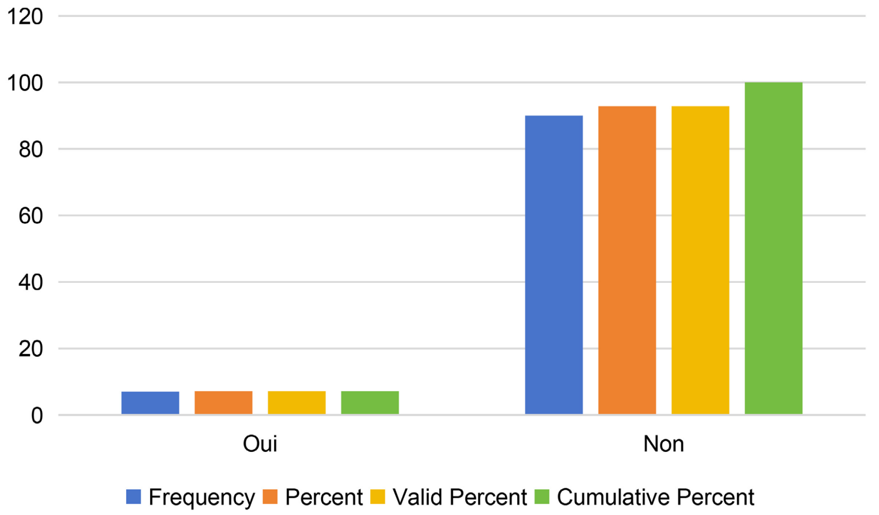


Figure 1. Proportion of use of AI in companies.

We see that 96.9 percent of IT security managers recognize the importance of using AI within their organization. There are only 3.1 percent who do not see the need. Anomaly detection is the prediction or detection of more or less suspicious behavior that may indicate malicious intent. AI offers a set of statistical tools which allows, among other things, to identify anomalies, either by feeding the algorithm with normal and abnormal examples (supervised learning), or by detecting outliers in relation to a behavior usual.

As we can notice in Figure 2, the perception of IA in Burkina Faso companies is higher despite the lack of use. Indeed, Artificial intelligence (AI), and in particular machine learning (ML), deep learning (DL) has seen huge pace in recent years and is now set to really start influencing all aspects of community and occupations in which people are engaged. This growth has been charged the advancement in computing power, combined with headway in algorithms and cybersecurity is no exception [6].

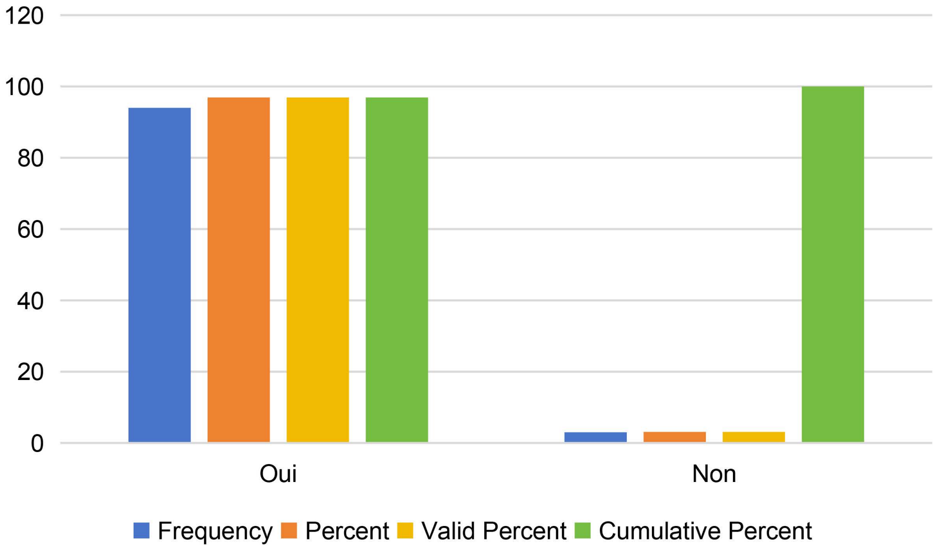


Figure 2. Statistics on the perception of AI within companies.

Figure 3 shows the statistic of the combination of the usage and perception of AI in the companies in Burkina Faso. With innovations in technology, the application of artificial intelligence (AI) in the area of commerce is rising to the top with an expected growing number of business transactions [7]. It shows how the AI is really important in your enterprise. Artificial intelligence (AI) and machine learning (ML) are increasingly being used for strengthening cybersecurity [8].

Simulation of an Attack on a Computer System Equipped with an AI

An attack using the Nmap tool gives the following results on the Darktarce AI.

Figure 4 shows the attack log, we have an example of an attack carried out that was responded to. This is the attack type Device/Attack and Reconnaissance Tools. In summary we have the description of the attack in question which is: a device uses common penetration testing tools. To this end the active solution to apply to this attack is given by Darktrace. This involves examining the device to see if it is a security device, these can be labeled as such to exclude them from future breaches. Non-security device activity merits further investigation into what else the device is doing and could pose a significant risk within the network.

Figure 5 shows the description of the attack here presented as: A device behaves abnormally and has violated a model with a very high score. In short we are dealing with an NMAP attack. Nmap (Network Mapper) is a powerful open source network analysis and security auditing tool. It is widely used by network administrators, security professionals and hackers for network exploration, vulnerability scanning and host discovery. Artificial intelligence advancements in the present day are proving to be the most effective method for preventing cyberattacks. Artificial intelligence (AI) is being used by experts as a protection

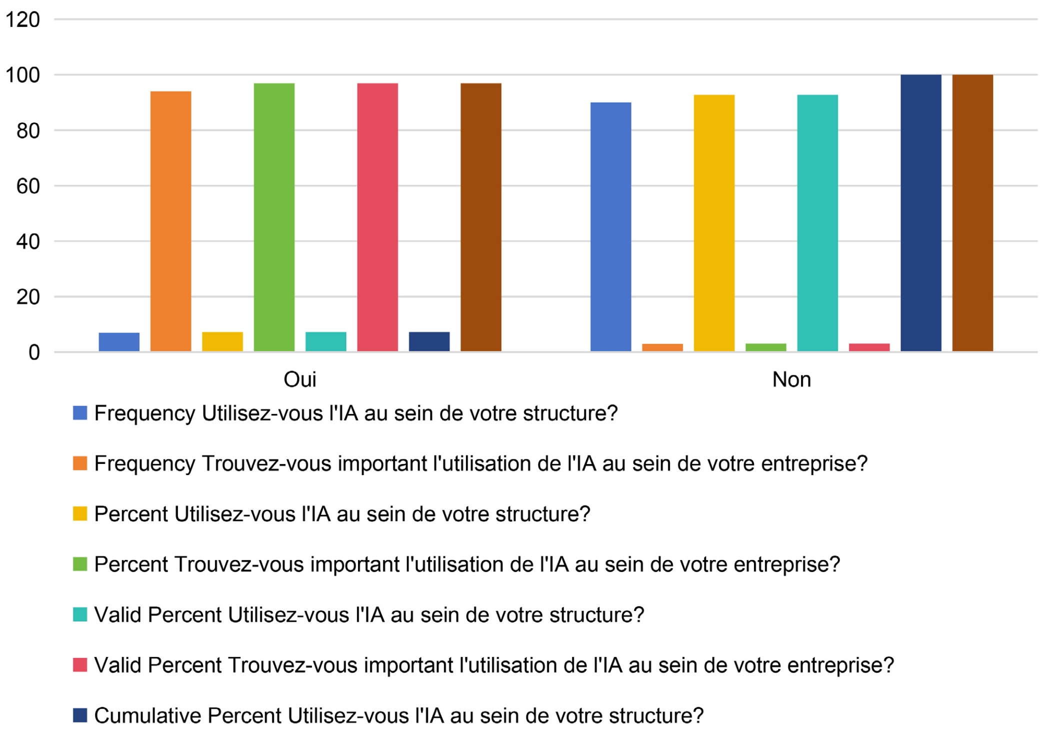


Figure 3. AI usage and perception statistics.

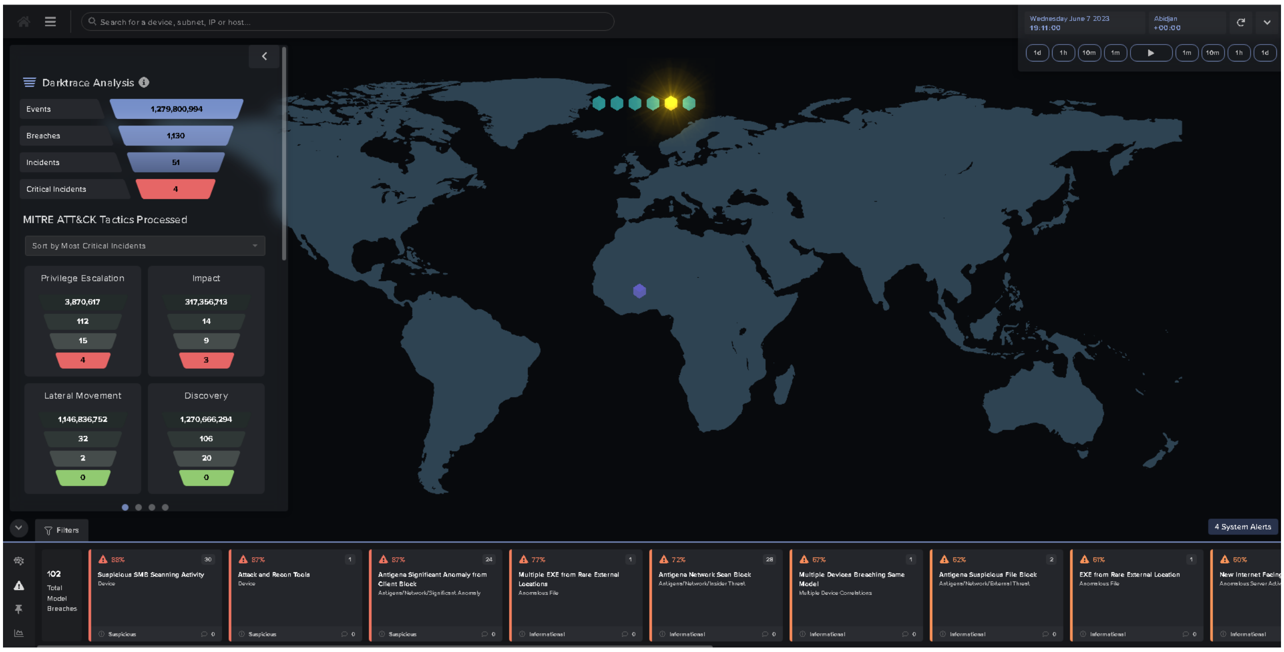
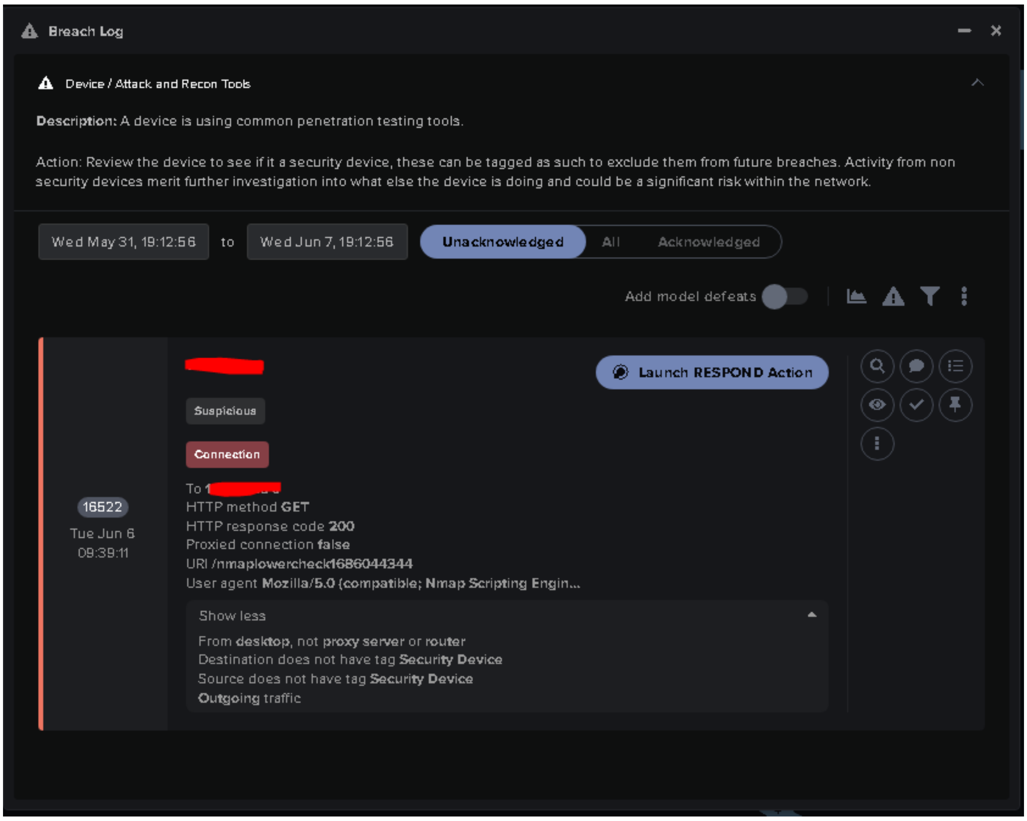

Search for a device, subnet, IP or host...
Wednesday June 7 2023
19:11:00
Abidjan
+00:00
1d
1h
10m
1m
1m
10m
1h
1d
Darktrace Analysis
Events 1,279,800,994
Breaches 1,130
Incidents 51
Critical Incidents 4
MITRE ATT&CK Tactics Processed
Sort by Most Critical Incidents
Privilege Escalation
3,870,617
112
15
4
Impact
317,356,713
14
9
3
Lateral Movement
1,146,836,752
32
2
0
Discovery
1,270,666,294
106
20
0
Filters
4 System Alerts
102 Total Model Breaches
88% 30 Suspicious SMB Scanning Activity Device Suspicious 0
87% 1 Attack and Recon Tools Device Suspicious 0
87% 24 Antigena Significant Anomaly from Client Block Antigena/Network/Significant Anomaly Suspicious 0
77% 1 Multiple EXE from Rare External Locations Anomalous File Informational 0
72% 28 Antigena Network Scan Block Antigena/Network/Insider Threat Informational 0
67% 1 Multiple Devices Breaching Same Model Multiple Device Correlations Informational 0
62% 2 Antigena Suspicious File Block Antigena/Network/External Threat Informational 0
61% 1 EXE from Rare External Location Anomalous File Informational 0
60% New Internet Facing Anomalous Server Activ Informational

Figure 4. Attack tools detected by Darktarce.

against cyberattacks. This technology is being used by security analysts to spot abnormalities, which reduces time and reduces total company expenditures [9].

Figure 6 shows us the attacking agent and the line circled in red allows us to understand the effectiveness of AI on computer attacks. This proves difficult in traditional systems.



Device / Attack and Recon Tools

Description: A device is using common penetration testing tools.

Action: Review the device to see if it a security device, these can be tagged as such to exclude them from future breaches. Activity from non security devices merit further investigation into what else the device is doing and could be a significant risk within the network.

Wed May 31, 19:12:56 to Wed Jun 7, 19:12:56

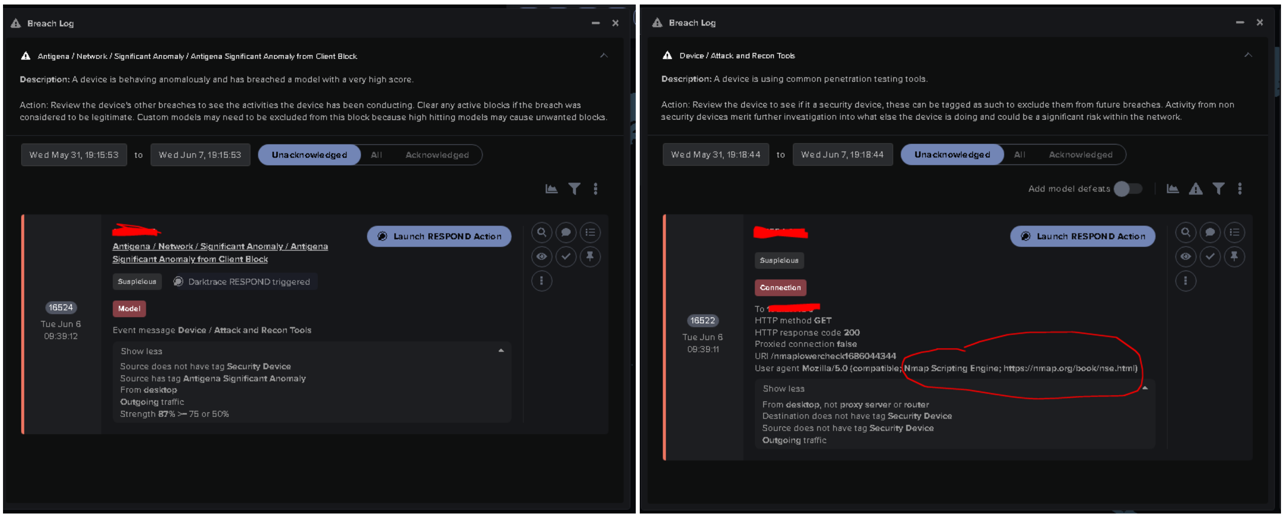
[redacted]

16522
Tue Jun 6
09:39:11

To [redacted]
HTTP method **GET**
HTTP response code **200**
Proxied connection **false**
URI **/nmaplowercheck1686044344**
User agent **Mozilla/5.0 (compatible; Nmap Scripting Engin...**

From **desktop**, not **proxy server** or **router**
Destination does not have tag **Security Device**
Source does not have tag **Security Device**
Outgoing traffic

Figure 5. DarkTrace response.



Antigena / Network / Significant Anomaly / Antigena Significant Anomaly from Client Block

Description: A device is behaving anomalously and has breached a model with a very high score.

Action: Review the device's other breaches to see the activities the device has been conducting. Clear any active blocks if the breach was considered to be legitimate. Custom models may need to be excluded from this block because high hitting models may cause unwanted blocks.

Wed May 31, 19:15:53 to Wed Jun 7, 19:15:53

[redacted]
Antigena / Network / Significant Anomaly / Antigena Significant Anomaly from Client Block

16524
Tue Jun 6
09:39:12

Event message **Device / Attack and Recon Tools**

Source does not have tag **Security Device**
Source has tag **Antigena Significant Anomaly**
From **desktop**
Outgoing traffic
Strength **87%** >= 75 or 50%

Device / Attack and Recon Tools

Description: A device is using common penetration testing tools.

Action: Review the device to see if it a security device, these can be tagged as such to exclude them from future breaches. Activity from non security devices merit further investigation into what else the device is doing and could be a significant risk within the network.

Wed May 31, 19:18:44 to Wed Jun 7, 19:18:44

[redacted]

16522
Tue Jun 6
09:39:11

To [redacted]
HTTP method **GET**
HTTP response code **200**
Proxied connection **false**
URI **/nmaplowercheck1686044344**
User agent **Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)**

From **desktop**, not **proxy server** or **router**
Destination does not have tag **Security Device**
Source does not have tag **Security Device**
Outgoing traffic

Figure 6. Agent attaquant outils nmap.

5. Conclusion

Cybercriminals are increasingly turning to artificial intelligence to attack on larger scales and evade detection. Business leaders surveyed say security strategies that rely on human intervention in the face of ever-changing and exponentially evolving attacks fail. It is therefore with this in mind that companies must quickly reform their strategies, be prepared to protect their digital assets and regain the upper hand over this new wave of fairly sophisticated attacks. Artificial intelligence is already useful in the fight against IT insecurity and should play a major role in the future. It is really important to say that Attacks to networks are becoming more complex and sophisticated every day. Beyond the so-called script-kiddies and hacking newbies, there is a myriad of professional attackers seeking to make serious profits infiltrating in corporate networks. Either hostile governments, big corporations or mafias are constantly increasing their resources and skills in cybercrime in order to spy, steal or cause damage more effectively. Traditional approaches to Network Security seem to start hitting their limits and it is being recognized the need for a smarter approach to threat detections such as AI [10].

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Kalinová, E. (2021) Artificial Intelligence for Cluster Analysis: Case Study of Transport Companies in Czech Republic. *Journal of Risk and Financial Management*, **14**, 411. https://doi.org/10.3390/jrfm14090411

[2] Boburbek, B., Sanjarbek, R., Elmurod, U. and Satimov, A. (2022) The Importance of Artificial Intelligence in Modern Technology. *Journal of Advanced Scientific Research*, **2**.

[3] Kunduru, A.R. (2023) Artificial Intelligence Advantages in Cloud Fintech Application Security. *Central Asian Journal of Mathematical Theory and Computer Sciences*, **4**, 48-53.

[4] Truong, T.C., Zelinka, I., Plucar, J., Čandík, M. and Šulc, V. (2020) Artificial Intelligence and Cybersecurity: Past, Presence, and Future. In: *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Springer, Singapore, 351-363. https://doi.org/10.1007/978-981-15-0199-9_30

[5] Santos, A.R. (2022) The Importance of Artificial Intelligence in Start-Up, Automation, and Scalation of Business for Entrepreneurs. *International Journal of Applied Engineering & Technology*, **4**, 1-5.

[6] Geluvaraj, B., Satwik, P.M. and Ashok Kumar, T.A. (2019) The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace. In: *International Conference on Computer Networks and Communication Technologies*: *ICCNCT* 2018, Springer, Singapore, 739-747. https://doi.org/10.1007/978-981-10-8681-6_67

[7] Zhuo, Z., Larbi, F.O. and Addo, E.O. (2021) Benefits and Risks of Introducing Artificial Intelligence in Commerce: The Case of Manufacturing Companies in West Africa. *Amfiteatru Economic*, **23**, 174-194. https://doi.org/10.24818/EA/2021/56/174

[8] Kshetri, N. (2021) Economics of Artificial Intelligence in Cybersecurity. *IT Professional*, **23**, 73-77. https://doi.org/10.1109/MITP.2021.3100177

[9] Krishnappa, T. (2023) A Review on Artificial Intelligence Techniques in Preventing Cyber Threats. *International Journal of Engineering Applied Sciences and Tech-*

nology, **8**, 185-189. https://doi.org/10.33564/IJEAST.2023.v08i01.029

[10] Veiga, A.P. (2018) Applications of Artificial Intelligence to Network Security. arXiv preprint arXiv:1803.09992.