MACHINE LEARNING-BASED INFORMATION SYSTEMS SECURITY MANAGEMENT

Svetlana Anđelić[1],
[0009-0001-3069-6702]
Velimir Dedić[2]*,
[0000-0002-8961-3529]
Nenad Dedić[2]
[0009-0003-3869-9187]

[1]Singidunum University,
Belgrade, Serbia

[2]Faculty of Information Technologies and Engineering - FITI,
Belgrade, Serbia

Abstract:
Modern companies' operations depend on the Internet and web services, so security concerns are critical. This paper discusses current security risks and responses, including security mechanisms. Risks specific to modern ages, especially financial institutions, can be categorized into ones due to increased use of mobile applications, break-ins of third-party organizations, and cryptocurrency usage risks. Protection mechanisms are used to protect corporate processes and data and must meet desired critical points. Further, this study presents specific operations of Darktrace, a suite of AI-powered software tools designed to protect corporate assets from cyberattacks. Darktrace uses both supervised and unsupervised machine learning algorithms to maximize threat detection performance, supporting the conclusion that artificial intelligence promises a lot in the realm of threat detection and intrusion detection.

Keywords:
Darktrace, Security risks, Protection Mechanisms, Machine Learning.

INTRODUCTION

Today's businesses depend entirely on the Internet and web services. As more and more people conduct daily financial and trade operations cashless, such activities are carried out through online payment sites, and credit transactions are completed online.

There are even greater dangers lurking online than in the so-called offline business; today, the major security risks stem from cyber fraud attempts and server hacking intended to obtain personally identifiable information (PII).

An entire computer network can attain a high degree of security by carefully managing the security of every component of that network, namely LAN and WAN, Data Centers, extranet, and Internet segments. To conclude, it is helpful to stress that IT-dependent business operations in a company are deemed secure only if all the individual components of the corporate computer network are adequately designed, managed, maintained, and monitored for intrusion and attacks.

Correspondence:
Velimir Dedić

e-mail:
velimir.dedic@fiti.edu.rs

DOI: 10.15308/Sinteza-2024-156-161

Timely prediction and detection of possible security threats have become an indispensable part of modern business on the web. Large corporations, especially those conducting online financial transfers, generally use several security tools to monitor and manage IS security.

In prediction and detection, machine learning and artificial intelligence have become the main backbone of many IS security software solutions.

2. SECURITY RISKS

Online financial transactions must be secure for the obvious reason: the protection of client assets. As cashless transactions grow, online payment sites manage required trade operations; even loans are handled online. In both situations, intercepted or otherwise compromised PII can be redirected and used for malicious activities.

If at least partially successful, a malicious action significantly affects the user involved and damages the company while trying to recover the data. The damage is financial; e.g., a company might be a victim of a ransomware attack and choose to pay to retrieve the compromised information, but the subsequent damage to corporate reputation and trust can be even more significant.

Online security issues that companies, especially banks, should consider are the following:

- Greater risk due to increased use of mobile applications-Today, many users access their bank accounts through mobile applications, most having minimal or no security. Therefore, banking software must be secured at the endpoints to prevent malicious activities.
- Break-ins of third-party organizations-As financial institutions have improved their cyber security systems, hackers have turned to shared banking systems and third-party networks to gain access. If such systems are not as secure as banks, attackers could gain indirect access more quickly than attacking a final victim directly.
- Increased risk of cryptocurrency hacking-The number of hacking attacks has also increased in the cryptocurrency world. It is difficult to set standards for cybersecurity systems implementation in this financial realm, for the business rules for cryptocurrency banking and financial operations are constantly changing. Thus, attackers are challenged and motivated to reach for significant illegal profits.

Security risks pose constant threats and must be carefully assessed, measured, and managed. A well-maintained security system must understand the threats it is exposed to, respond to them, and learn from the attacks it survives.

3. PROTECTION MECHANISMS

We use protection mechanisms to implement layers of trust between system security levels. Trust levels are used "to provide a structured way to compartmentalize data access and create a hierarchical order to make a protected system more manageable." [1] The protection mechanisms are used to protect processes and data and have one of the following forms:

- Layering
- Abstraction
- Data Hiding
- Encryption

When looking at the current state of internet security, one must think daily about improving online application protection mechanisms. Here are some critical points to look out for in the world of business financial software development: [1]

- Security Systems Audit

A thorough security audit of a firm's information system is highly recommended before implementing new cybersecurity software. Through inspection and control, the strengths and weaknesses of the existing setup are revealed, and recommendations are also given to optimize investment into a new system.

- Using a firewall

Managing cyber security in companies is not a software-only business. Adequate hardware, namely firewall devices, is also required to block attacks. With an updated and well-tuned high-end firewall installed, companies can block malicious activity before reaching inner network parts.

- Antivirus and anti-malware applications

Although upgrading the firewall increases protection, outdated antivirus and anti-malware software can be a dangerous weakness. In addition, although aged software might have implemented the latest rules and virus signatures, it could fail to recognize and prevent an attack with possibly catastrophic consequences; therefore, regular security software updates are necessary.

- Multi-factor authentication

Multi-factor authentication (MFA) is highly critical to protecting customers who use mobile or web e-banking applications. Many such users never change their passwords; if they do, they make insignificant changes. Deploying MFA prevents attackers from reaching the network because it requires another layer of protection, e.g., a combination of a password and a six-digit code sent to the user's mobile phone.

- Biometrics

This is another, more secure version of MFA. This authentication relies on retina scans, fingerprints, or facial recognition to confirm the user's identity. Today, biometrics systems are very complicated to hack.

- Automatic logout

Many websites and applications allow a user to remain logged in regardless of the inactivity of the current session. Even worse, the password is usually saved and never re-entered; therefore, users can access the system anytime without entering login credentials. However, this also allows attackers to intrude easily. Automatic logout minimizes this by closing user access after a predefined inactivity period.

- Education and training of employees and users

The above measures can increase cyber security in the financial and banking sector. However, those are ineffective if customers continue to access the system from unsecured locations or improperly manage access to their login credentials. Corporate education is essential both for employees and users of applications. When a company informs its customers of the consequences of misbehavior, it might encourage clients to change their risk-prone habits.

To conclude, today's secure systems are designed as layered detection and defense mechanisms structured to implement the requested security policy goals.

4. DARKTRACE-AN ILLUSTRATION OF THE AI-BASED SECURITY SYSTEM OPERATIONS

Darktrace is a suite of AI-powered software tools that learns about details of a user's specific environment, building a unique defense system able to detect any deviation and respond if a vulnerability or threat is indicated.

The principles of operation for the Darktrace system are twofold: it uses both supervised and unsupervised machine learning algorithms to maximize threat detection performance.

Gradually, the system learns about usual and expected traffic patterns in a network. Darktrace finds out what "normal" network behavior is. This conclusion does not depend primarily upon knowledge of previous attacks. It thrives on the scale, complexity, and diversity of modern businesses driving the network traffic itself, where every device and person is unique. Datktrace turns the innovation of attackers against them – any unusual activity is visible, and assumptions about behavior are constantly revised using probabilistic models. The architecture of the Darktrace system is shown in Figure 1.

For each interaction in a specific environment, Darktrace questions: is this normal behavior? – and forms answers based on raw data stream and data features enhanced by artificial intelligence (AI) (Figure 2). Understanding the specific environment is crucial in illuminating and disrupting the entire spectrum of cyber threats, from new attacks to insider threats. Self-learning AI is behind every component of the Cyber AI Loop, powering customized, comprehensive, and continuously evolving security solutions based on mathematical models unique to each organization.

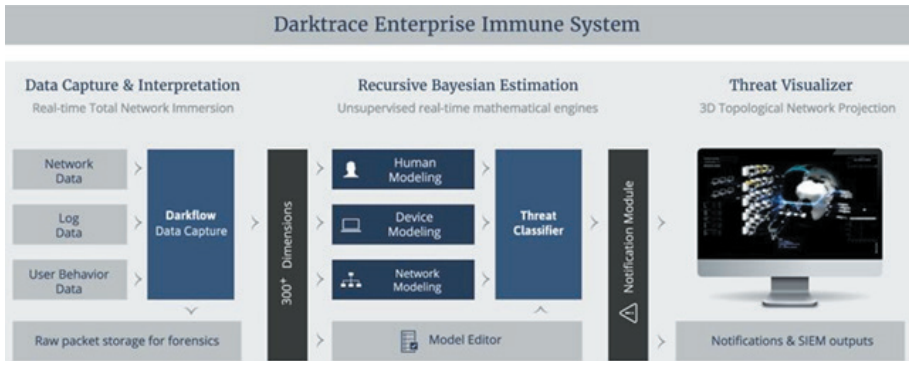

Figure 1. Darktrace architecture [2].

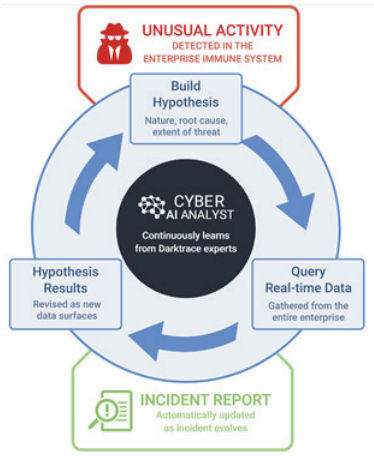

Figure 2. Cyber AI Analyst continuously builds and tests hypotheses, reasoning to conclusions at machine speed and scale [3].

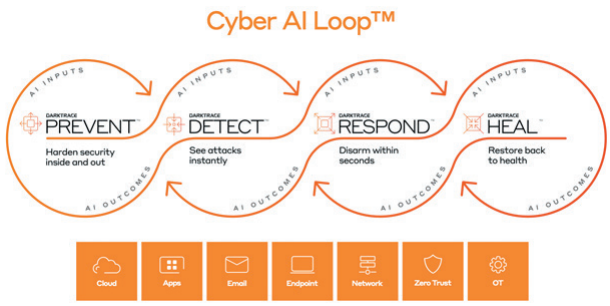

Figure 3. Components of Darktrace [4].

Darktrace performs the task of strengthening the defense from the inside and the outside threats, and it consists of the following functional components (Figure 3):

- Darktrace PREVENT - empowers security teams to reduce cyber risk by prioritizing vulnerabilities and proactively strengthening defenses;
- Darktrace DETECT - insight into threats and attacks in real-time;
- Darktrace RESPOND - by understanding the environment adapted to a specific organization, it uses it to take precise and targeted action by interrupting cyber-attacks;
- Darktrace HEAL – enables recovery in a cyber attack by restoring the system to a reliable operating state.

The following describes the application of the Darktrace tool in a company whose identity will not be disclosed due to data sensitivity. The company operates in several European countries, including Serbia.

A server installed on the company premises and placed in one of the data center (DC) server zones resides behind the DC firewall.

The Darktrace server is given access to other servers and workstations within the corporate domain, where it scans in real-time and detects any unexpected behavior of hosts in the network, i.e., one that deviates from the usual.

By starting the Network scan option, Darktrace starts to scan the network and hosts that are active at that moment and have open connections and live traffic. Figure 4 shows the result of a scan performed by Darktrace in a short time as it scans and analyzes traffic from available hosts.

After completing the scan, the system swiftly singles out one of the hosts exhibiting unusual behavior. The host destination is detected by IP range, and the country where the host resides is shown (Figure 5).

Darktrace (DT) singles out the connections of the suspicious host and begins to analyze the traffic it generates in more detail (Figure 6). In addition to regular traffic such as DNS and traffic related to certain Microsoft services (Teams, etc.), BitTorrent activity was also detected.

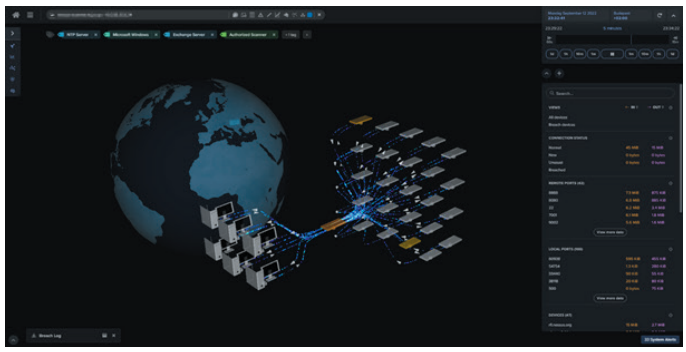

Figure 4. Darktrace network scan.

Figure 5. Targeting a single host with unusual behavior.

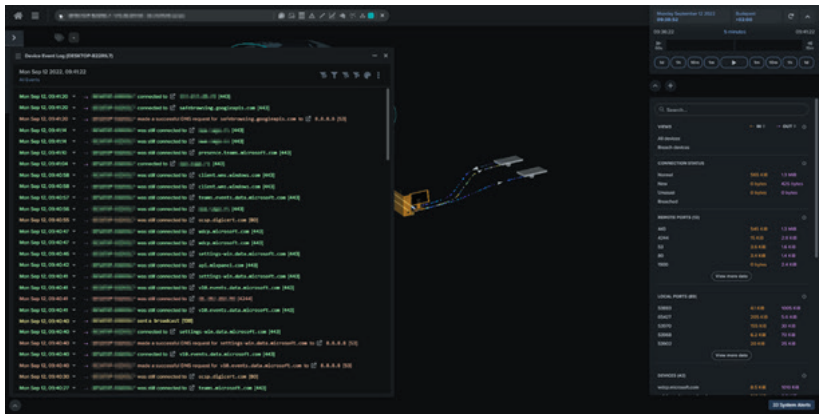

Figure 6. Isolating host connections with unusual behavior.

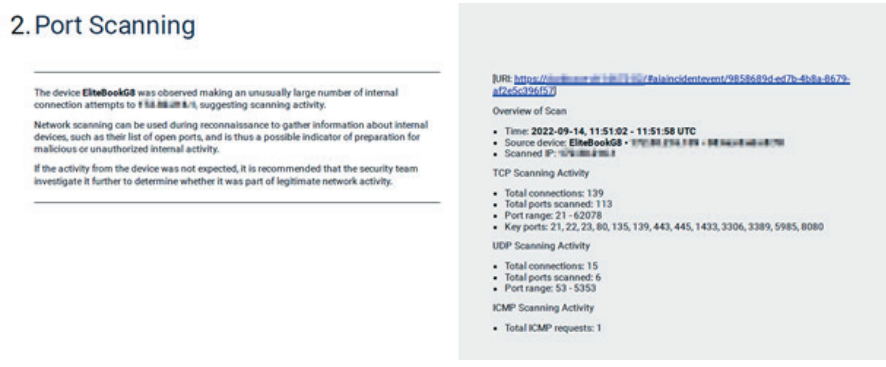

Figure 7. Detecting multiple dedicated host connections and BitTorrent activity.

The detailed log shows the exact data on the number of connections, the ports through which it communicated, the type of network connection, and the web address of the site it was connected to perform BitTorrent activities [5]. (Figure 7).

5. CONCLUSION

The full potential of artificial intelligence, i.e., its application in all spheres of private and business life of most individuals, will come to the fore in the next few years.

There are many questions about the ethics of its application in certain areas, but what is certainly inevitable is that it has great potential in the IS security sphere, especially from the aspect of monitoring and managing IS security risks and threats.

Artificial intelligence promises a lot in the realm of threat detection and intrusion detection. Several features of machine learning algorithms make a perfect fit for security mechanism designs: the unique ability to detect previously unknown and unused threats, automated response recommendations, and self-regulation security policy updates, which are platforms for improving current security mechanism implementations.

Of course, when judging the overall security improvements, one must never neglect the importance of the human factor, corporate process modeling, security policies, risk management tools, and assessments, besides the immense significance of purely technical factors improvements, where AI offers vast potential in the future.

6. REFERENCES

[1] "Understanding Protection Mechanisms," 2024. [Online]. Available: https://www.oreilly.com/library/view/cissp-training-guide/078972801X/078972801X_ch03lev1sec8.html. [Accessed 04 22 2024].

[2] P. Khatri, "The importance of cyber security in banking," 25 September 2019. [Online]. Available: https://www.theglobaltreasurer.com/2019/09/25/the-importance-of-cyber-security-in-banking/. [Accessed 17 March 2024].

[3] S. Sangeeth, "Machine learning in CyberSecurity – A Darktrace case study," 19 October 2019. [Online]. Available: https://www.linkedin.com/pulse/machine-learning-cybersecurity-darktrace-case-study-sangeeth-sahana/. [Accessed 17 March 2024].

[4] "Darktrace Cyber AI Analyst, white paper," January 2021. [Online]. Available: https://em360tech.com/sites/default/files/2021-01/Darktrace%20Cyber%20AI%20Analyst.pdf. [Accessed 20 March 2024].

[5] "What is Machine Learning?," [Online]. Available: https://darktrace.com/cyber-ai-glossary/machine-learning. [Accessed 20 March 2024].

[6] "What is BitTorrent (BTT) and How Does it Work?," 19 February 2023. [Online]. Available: https://www.gate.io/learn/articles/what-is-bittorrent/401. [Accessed 25 March 2024].