ADEO
CYBER SECURITY

2024 Threat Report

TABLE OF CONTENTS

With ADEO;

It is widely accepted that companies and institutions cannot solve their cybersecurity problems alone and can only succeed with the right ally by their side. ADEO Cyber Security was established in 2008 with the understanding to provide services in all areas of technology, expertise, and processes that companies and institutions will need to develop active cybersecurity defense strategies.

ADEO stands alongside its customers as a reliable ally in cybersecurity, devising and implementing strategies to strengthen cybersecurity defenses. With a focus on maximizing efficiency, ADEO offers comprehensive cybersecurity services based on a 24/7 principle, including deep expertise in offensive and defensive cybersecurity, cyber resilience capabilities, and technology procurement.

With a team of over 160 experts who are well acquainted with their clients' infrastructures and have intervened in numerous cyberattacks against these infrastructures before, ADEO provides services in

- Managed Cybersecurity Services,
- Cyber Resilience and
- Governance Risk and Compliance

offering a wide range of competencies.

Active Not Passive

Attackers are now avoiding the use of malware. In nearly 70% of detected attacks, no malware is used. Therefore, it is necessary to move beyond signature-based passive technologies to actively advocated processes that provide high visibility, supported by cybersecurity experts.

Dynamic Not Static

Attackers are now moving much faster. The time from initial access to compromise of a system has decreased to an average of one and a half hours. This situation emphasizes the importance of a protection approach based on dynamic threat hunting fueled by cyber intelligence.

Continuous Not Intermittent

Cyber attacks can occur at any time of the day. In fact, it is known that cyber attackers specifically choose off-hours to reduce the risk of resistance against the attack. Therefore, it is crucial to operate cybersecurity processes 24/7.

ADEO Managed Detection and Response (MDR) Service

MDR remotely monitors, detects and responds to threats detected within your organization. For this, the service provider uses an endpoint detection and response (EDR*) tool, which provides the necessary visibility into security events at the endpoint.

After providing the required visibility, telemetry data from endpoints is collected in the center console. Here, with the help of threat intelligence data and advanced analytics, suspicious incidents are detected and responded quickly.

This tools;

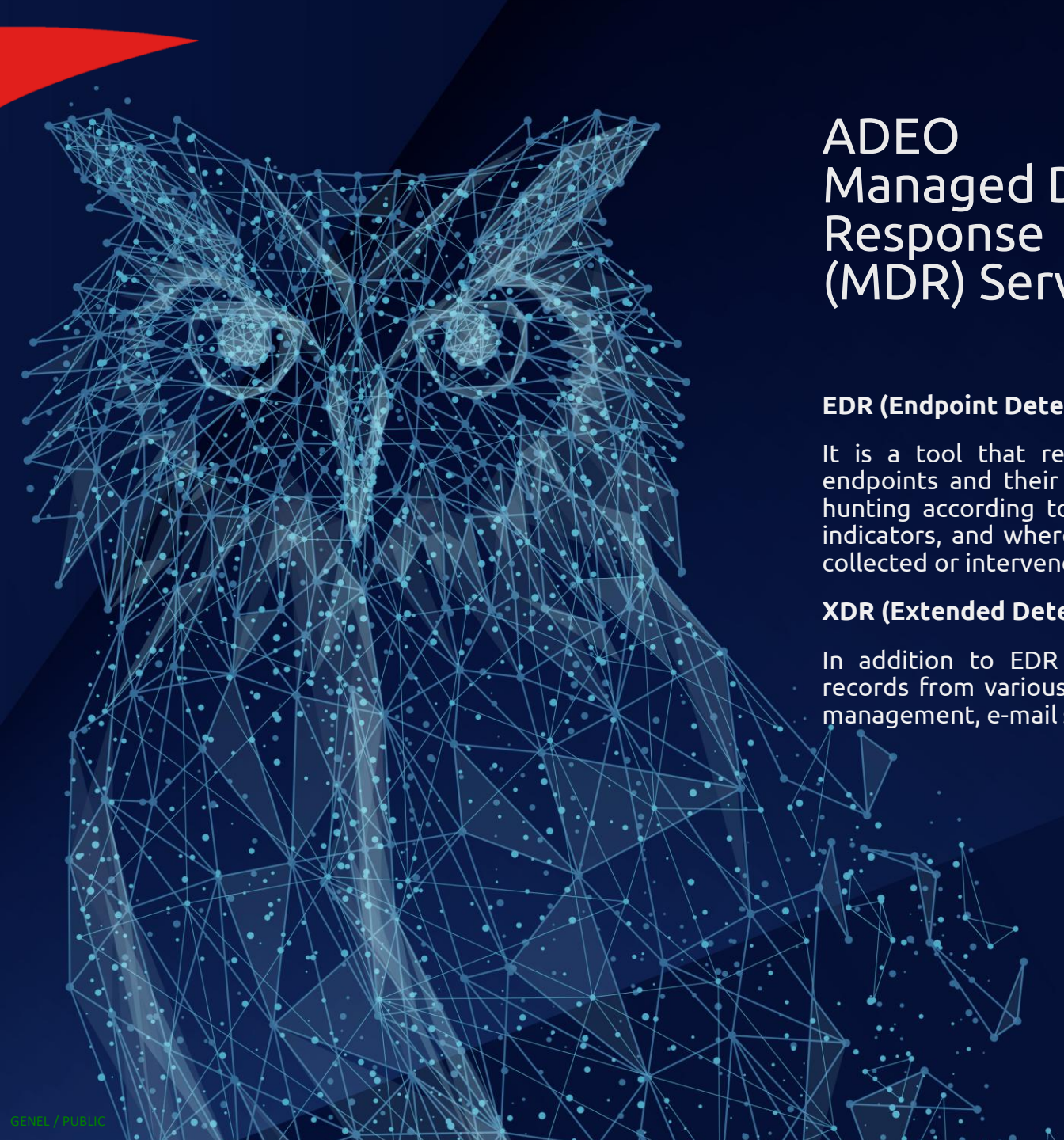
- allow attacks detected by the MDR team to be highly accurate.
- provide a detailed view of what happened before and after the relevant cyber incident.
- allow planning actions to quickly prevent a similar attack immediately after a Cyber attack.

In this way, institutions gain resistance against both known and unknown cyber attacks.

MDR Analysts can detect real-time cyber incidents and take very fast action regarding these detected cyber attacks.

Fast verification and action capabilities are of critical importance in the response of advanced cyber attacks.

"**MDR** is a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring and response."



ADEO Managed Detection and Response (MDR) Service

EDR (Endpoint Detection and Response)

It is a tool that records all the processes running at the endpoints and their activities, provides detection and threat hunting according to behavioral indicators as well as atomic indicators, and where evidence of suspicious activities can be collected or intervened when necessary.

XDR (Extended Detection and Response)

In addition to EDR tools, they are tools that can analyze records from various sources such as network, cloud, identity management, e-mail security.

ADEO 2024 Threat Report: Cyber Security Analysis of2024

This report is the result of a comprehensive analysis prepared by ADEO, a leading figure in the field of cybersecurity, based on its experience in the sector in 2024. Its aim is to assist security professionals, businesses, and individuals in understanding the security threats we face.

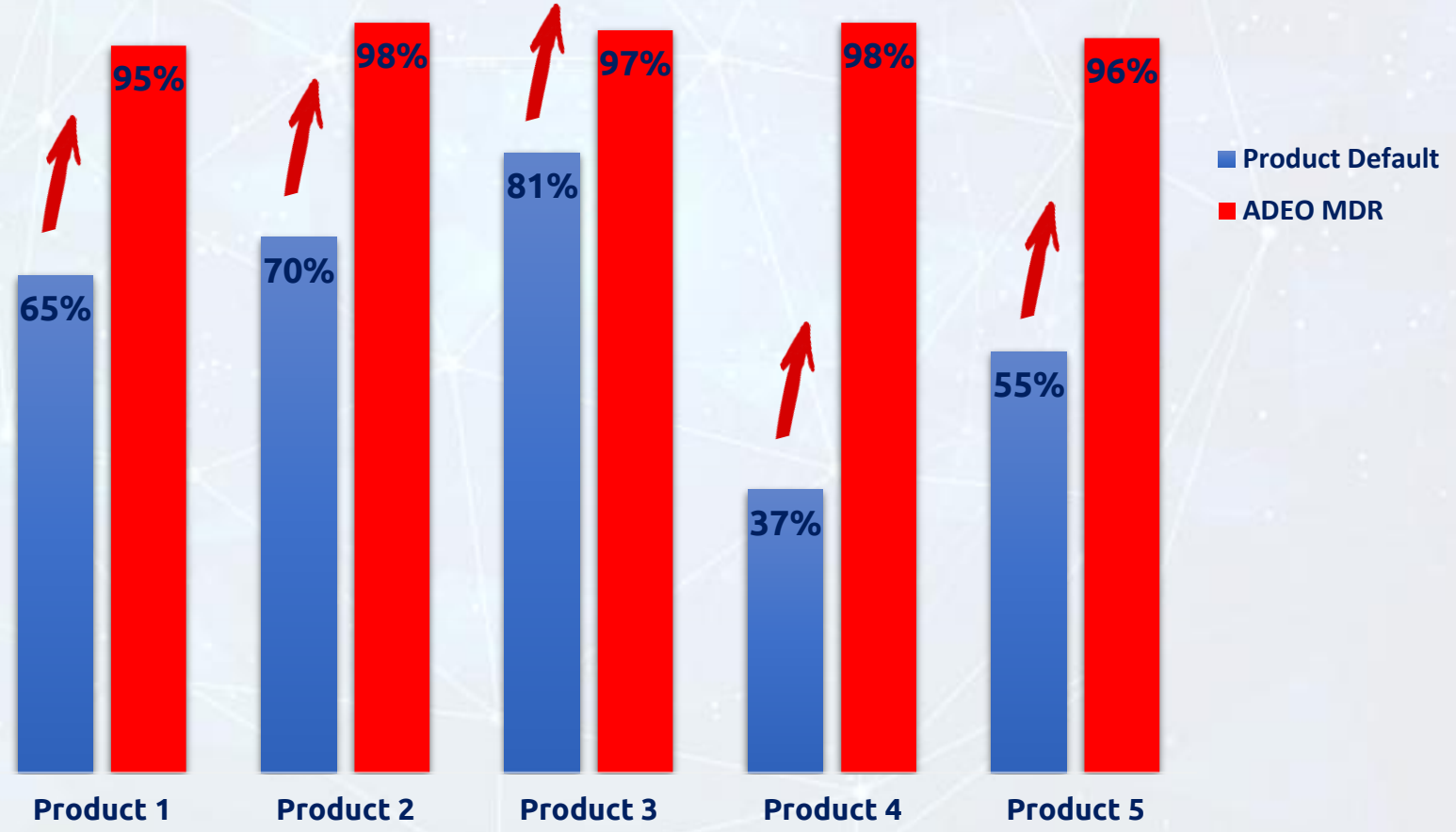
The report provides detailed information on identifying significant threats, how they emerge, and measures that can be taken to manage future risks.

ADEO 2024 Threat Report has been prepared by an expert team to help organizations and individuals strengthen their cybersecurity defenses and develop awareness and measures to protect their digital assets.

What Did We Do in 2024?

Adeo MDR Team **has consistently improved the detection capabilities** of the EDR/XDR solutions used by its protected customers through its specially developed rules.

The extent to which the detection mechanisms of EDR/XDR, which are undergoing improvement efforts, increase in effectiveness after configuration activities and the addition of rules to the system is presented graphically.



Most Targeted Sectors and Their total Number of Incident in 2024:

Holding
4

Aviation
4

The Busiest Day in 2024:

ALARM:
Warning messages falling on security tools used to detect cyber attacks are called. These alarms are grouped according to their criticality level.

27 June

Number of Alarms Reviewed This Day

5969

Total Number of Rules Developed

The number of rules, which was **5000** in January 2024, was increased to **5,500** by the end of the year.

The number of IOCs, which was **120,000** in January 2024, was increased to **175,000** by the end of the year.

The number of IOCs scanned with threat intelligence from internal and external sources: **175,000**

Most Used Initial Access Technique

Initial Access Technique:
By taking advantage of various vulnerabilities, the attacker gains the initial access to the system and starts to use other tactics and techniques by reaching the targets.

Phishing

%64,28

Daily Routine of MDR Team

According to the obtained data, **99.8%** of the analyzed alarms were examined by the ADEO MDR team without notifying the customer, and the necessary intervention procedures were applied based on the maturity of the product used.

An average of **5 new detection rules** are written daily by **ADEO MDR** team.

Tightening/improvement works are also carried out in accordance with the rules determined as false positive.

0.02% of the alarms were confirmed, and necessary actions were taken after approval.

The detected **IP** and **Domain** are checked by the **intelligence services** and the **IP blocking** process is performed by examining the machines with which it is in communication within the network.

As a result of **detection of malware**, activities are examined with a **threat hunting** approach, machines spreading malware are **isolated** and **necessary actions** are taken.

TRUE POSITIVE ALARM:
These are alarms that indicate a real attack or unwanted/illegal behavior.

FALSE POSITIVE ALARM:
These are the alarms that are determined as a result of the analyzes that do not indicate a real attack or that occur in accordance with the wrongly written rules.

Managed Detection and Response Incident Management Stages

INCIDENT

They are attacker activities that require in-depth analysis and incident response processes as a result of the analysis of a detected real alarm.

Incident response procedures are required as a result of some initial access techniques, such as attackers exploiting zero-day vulnerabilities or obtaining employee password/username information.

ADEO MDR team **researches** and **detects compromised machines**.

The MDR detection phase involves detecting and identifying suspicious activity on systems.
The mean detection time (Dwell Time) of possible **high severity** and **critical** anomalies determined by using security products such as **EDR**, **NDR**, **SOAR** and the competencies of MDR Analysts is **5 minutes 55 seconds**.

Suspicious activities detected through various security products are examined in detail by **ADEO MDR** Analysts **7x24x365** days.

The response phase is the actions taken to **stop** and **prevent** the activities detected as malicious as a result of the analysis and to **prevent the activity from spreading** within the organization.
In **2024**, the mean **response time** of **ADEO MDR** team to **high severity** and **critical** incidents was **15 minutes 41 seconds.**

The recovery phase includes measures to **eliminate, improve**, and **prevent repetition** of threatening situations

Number of Incident Response

14

INCIDENT MANAGEMENT STAGES

SECURITY BREACH DETECTION ANALYSIS RESPONSE REMEDIATION

Detection and Response Time

Mean Time to Detection
5m 55s

Mean Time to Response
15m 41s

Annual Alarm Numbers and Levels

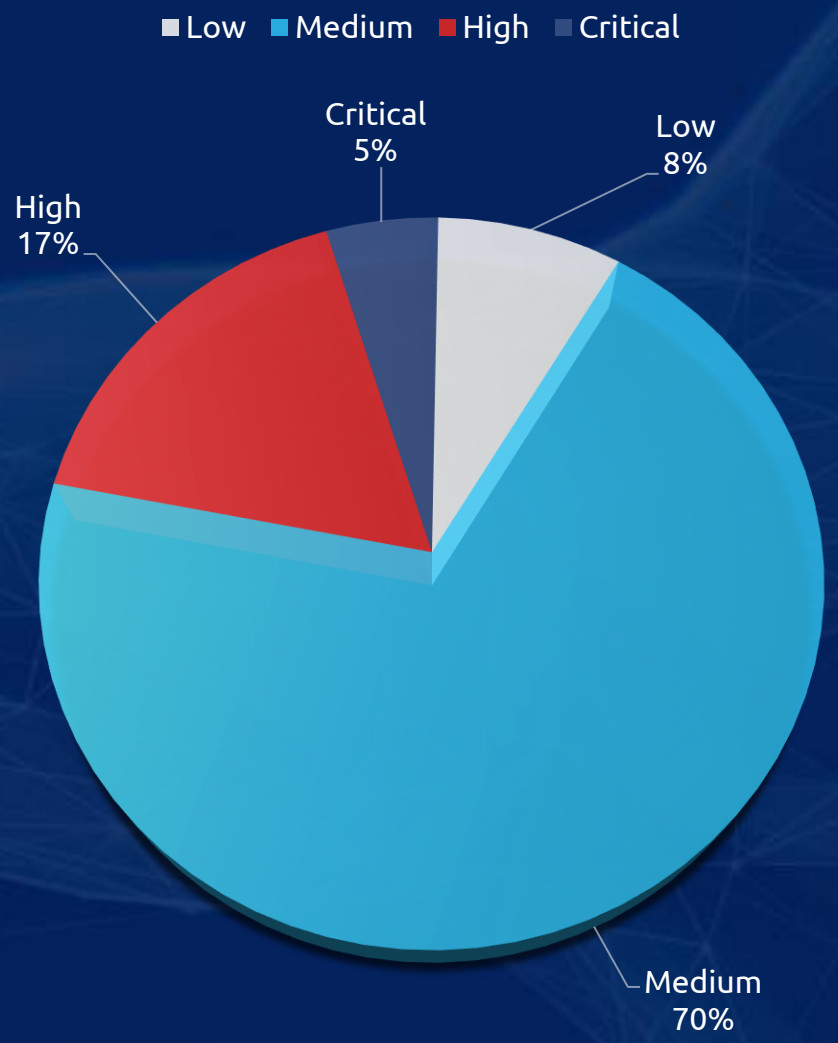
In 2023, the highest number of alarms received on a single day was **3886**, while this number was reported as **5969** on the busiest day of **2024**.

ADEO's rule development and improvement efforts are continuously ongoing.

Within the scope of these works, **the target for 2025** is to reduce the number of critical and high-level alarms and to increase the number of true positive alarms.

Annual Alarm Numbers and Levels

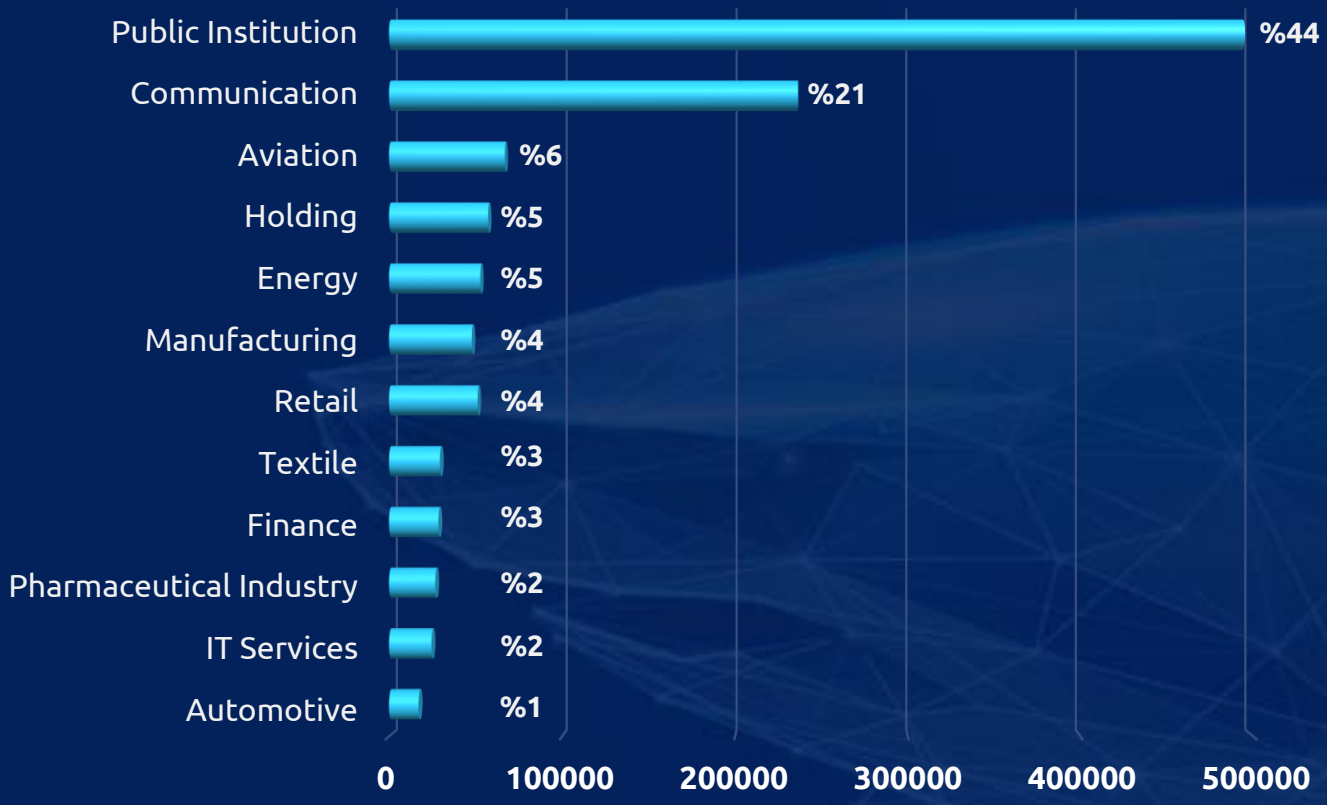
The mean detection time of only high severity and critical alarms was **5 minutes 55 seconds**, and the mean response time was **15 minutes and 41 seconds**.



DETECTION TIME:
It is the time elapsed between the realization of the attack and the detection of the attack by the MDR team and defining it as an attack.

RESPONSE TIME:
It is the time interval when the attack occurs, and the necessary action is taken after the relevant attack is seen and defined by the MDR Team.

Distribution of Alarms by Sectors



The Sectors with the Most Alarms Observed

COMMUNICATION:
Telecommunication and internet services form the backbone of all other sectors' infrastructure. Service disruptions can have large-scale consequences, and this sector is frequently targeted by DDoS attacks, data breaches, and unauthorized access attempts. Moreover, protecting user data and communication networks is crucial for national security.

For these reasons, the public and communication sectors are among the primary targets of cyber attackers and continuously face evolving threats.

PUBLIC INSTITUTION:
Government institutions store vast amounts of sensitive citizen data and manage critical infrastructures, making them attractive targets for state-sponsored attacks, espionage attempts, and ransomware. Additionally, legacy technologies and extensive network structures in public systems provide further opportunities for attackers.

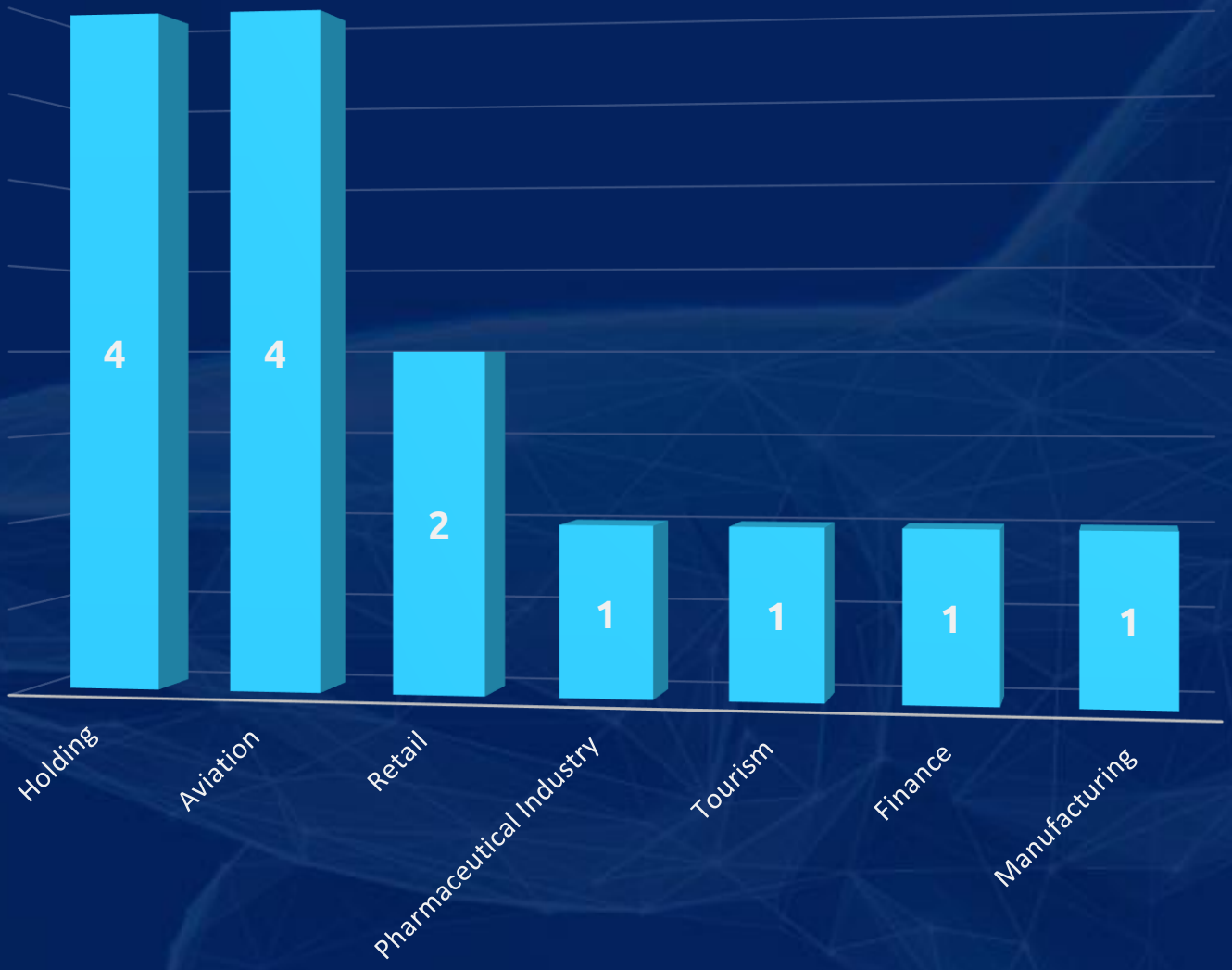
Sectors with the Highest Number of Incidents

Why Holdings&Aviation Sector?

The aviation sector has been targeted by cyber attackers due to its critical infrastructure, high-value data, and the significant impact of operational disruptions.

Holdings, on the other hand, are attractive targets because of their extensive operational networks, financial resources, and subsidiaries.

Additionally, challenges in supply chain security and attacks leveraging employees further increase risks in these sectors.



Important Security Vulnerabilities Experienced in 2024 and ADEO MDR Service's Detection Rules by Numbers

The rules we wrote as **ADEO MDR** about the important **Top 20+** vulnerabilities published in **2024** and the number of **IOCs we added** are shown in the table on the next page. As can be seen here, the number of cyber incidents is increasing day by day.

When we go into the details of the cyber attacks that occurred, the detection rate of these attacks is lower than the detection rate of previous attacks. In addition to the products' own detection capabilities, **proactive security solutions are needed** for the detection of new attacks.

"Proactive security solutions are needed for the detection of new attacks."

At this point, it is ensured that the threat indicators obtained as a result of regular research from **cyber threat intelligence sources are blocked, the attacks obtained from these sources are analyzed, the rules for the detection of the related attacks are developed and the written rules are tested in our laboratory environments**, added to the ADEO rule database and disseminated on our customers' systems.

Our threat detection and intelligence analysts regularly conduct research on **emerging security vulnerabilities**. After the vulnerabilities are technically examined and tested in laboratory environments, **more than one rule set** is developed to increase the visibility of the attack surface, specific to **the detected IOCs** and the different observed patterns.

Important Security Vulnerabilities Experienced in 2024 and ADEO MDR Service's Detection Rules by Numbers

Security Vulnerability	Number of Rules Written	Number of IOCs Added
AnyDesk Hacked - Signature	4	30
Lockbit Targeted Turkey in March	15	230
CVE-2024-3094 XZ Backdoor	2	63
CVE-2017-3506 Oracle WebLogic	-	87
CVE-2024-4577 PHP - CGI Argument Injection	-	116
CVE-2024-6387 RegreSSHion Vulnerability	5	34
APT40 Advisory by FBI	5	10
Void Banshee APT Exploits Microsoft Zero-Day in Spear-Phishing Attacks	3	11
China-linked APT17 Targets Italian Companies with 9002 RAT	2	8
FIN7Cybercrime Gang EDR Bypass	3	119
APT41 Has Arisen From the DUST	9	28
New ShadowRoot Ransomware Attacking Business Via Weaponized PDF's	5	22
Kematian Stealer	4	20
CROWDSTRIKE_BSOD_scams	1	355
BlankBot Banking Trojan	-	20
2018-0824 RCE Vulnerability exists in "Microsoft COM for Windows"	-	76
Palo Alto Networks PAN-OS CVE-2024-0012 and CVE-2024-9474	-	20
CVE-2024-47575 FortiManager Zero-Day Exploitation	-	5
CVE-2024-28986 SolarWinds Web Help Desk (WHD) Java Deserialization RCE	1	-
CVE-2024-38063 Windows TC/IPv6 RCE	1	-
CVE-2024-6409 Red Hat Enterprise Linux 9 OpenSSH	-	28
Brokewell Banking Trojan	-	32

Rule Studies of ADEO MDR Service in 2024

With the rules developed about the relevant security vulnerabilities and attacks and the competencies of MDR security analysts, **threat hunting** is carried out on our customers' systems at regular intervals. Before potential cyber attacks occur, the relevant vulnerability or attack indicators are detected.

After the determination made, the necessary precautions and actions are taken, and the institution is informed about the subject. Attack-related rules are added to customer systems and **monitored** by **MDR security analysts** for **7x24x365** days. Details of the findings are shared with our customers through MDR reports on a regular basis.

“Attack-related rules are added to customer systems and monitored by MDR security analysts for 7x24x365 days.”

After a certain period, after the rules are added to the customer systems that are monitored by **security analysts**, the alarms regarding the exploitation of the relevant vulnerability are detected by the analysts. In line with the investigations, after the exploitation of cyber attacks is prevented by the developed rules and IOCs, the **root cause** causing the vulnerability is **investigated by the analysts**.

ADEO threat intelligence resource is updated with the **findings** and **IOC data** obtained after the analysis. The intelligence data sets obtained from the attacks are added to our customers' systems on a regular basis. In this way, with the added IOC and intelligence data, the exploitation of the relevant security vulnerability on all customer systems is prevented.

Rule Studies of ADEO MDR Service in 2024

In these days when attackers can penetrate systems and establish persistence in a matter of minutes, whether targeted or untargeted, the most effective method to mitigate such threats is a Managed Detection and Response (MDR) service staffed by knowledgeable, skilled, and experienced MDR analysts. The primary task of an MDR service is to detect threats as quickly as possible and then minimize the impact of the threat through rapid and accurate intervention.

XDR/EDR products are our most powerful weapons in this relentless cat-and-mouse game with modern attacks and attackers. To succeed in this battle, detection and response times with EDR/XDR products need to be reduced to **below 20 minutes.**

Although today's EDR/XDR solutions are quite successful in detecting cyber threats and attacks, unfortunately, they are not sufficient.

As a result of the work conducted by ADEO MDR team, it has been determined that the detection mechanisms of EDR/XDR need improvement. It is highly crucial to enhance and keep up-to-date EDR/XDR solutions according to the structure of the organization, potential threats, and attacks they may face, perform best configuration practices, and especially add EDR/XDR rules targeting current threats to the systems.

The EDR/XDR rules created using the tactical and operational cyber threat intelligence gathered from hundreds of cybersecurity incidents intervened by the ADEO DFIR team and the analysis of alarms generated by hundreds of thousands of endpoints monitored under the ADEO MDR service significantly enhance the effectiveness of these detection mechanisms.

As a result, ADEO MDR and DFIR teams significantly increase detection levels and can reduce detection and investigation times to below 6 minutes by utilizing accurate and precise information obtained directly from the field and through the creation of EDR/XDR rules.

Rule Studies of ADEO MDR Service in 2024

Proactive Approach in Cybersecurity: ADEO MDR Team

In today's digital world, cybersecurity is of critical importance. Cyber attacks are increasing and becoming more complex with each passing day. Therefore, adopting a proactive approach to cyber threats is vital.

As ADEO, we place great emphasis on cybersecurity. We offer Managed Detection and Response (MDR) services to protect our customers against cyber attacks. Our MDR team closely monitors every vulnerability that arises and continuously develops rules to detect undetected attacks.

Through the developed rules, **we proactively protect our customers and ensure that their systems remain up-to-date.** This way, we minimize the risks such as data loss, financial loss, and reputation damage that cyber attacks can cause.

Benefits of ADEO MDR Team's Proactive Approach:

Faster Detection and Response:
Our team utilizes advanced threat hunting techniques and artificial intelligence to detect cyber attacks more quickly and intervene immediately.

Better Protection:
Due to continuously updated rules, our customers are protected against the latest cyber threats.

Reduced Risk:
Our proactive approach minimizes the risks that cyber attacks can cause.

More peace of mind:
Our customers can focus on their business with the comfort of knowing that their cybersecurity is being protected by ADEO's expert team.

Rule Set Sustainable Growth and Maturity Analysis: ADEO 2024 Perspective

When we examine the rule set development of our cybersecurity infrastructure, a parabolic increase has been observed in previous years.

2021: From 600 to 2,000 (233% increase)
2022: From 2,000 to 4,000 (100% increase)
2023: From 4,000 to 5,000 (25% increase)
2024: From 5,000 to 5,500 (10% increase)

This slowing growth trend is actually a natural result of our rule set's maturation process.

The initial rapid growth was driven by the need to cover fundamental threats and establish a broad defense spectrum.

The lower increase rate observed in 2024 **(10%)** indicates that our rule set has reached an optimized maturity level.

The Key Reasons Behind This Slowing Growth:

- ✓ **High detection rate of existing rules,**
- ✓ **Comprehensive coverage of the MITRE ATT&CK framework,**
- ✓ **Minimization of false positive rates,**
- ✓ **Successful outcomes from rule optimization and refinement efforts.**

Our New Focus Is Not on Increasing the Number of Rules, but Rather:

- ✓ **Optimizing the effectiveness of existing rules,**
- ✓ **Adding targeted rules for emerging threat vectors,**
- ✓ **Enhancing correlation between rules,**
- ✓ **Further improving detection quality.**

This approach maximizes the efficiency of our cybersecurity operations while minimizing unnecessary alert fatigue.

The maturity level our rule set has reached enables us to establish a more sustainable and effective cybersecurity infrastructure.

#Top 5
Agenda of 2024

Top 5 Agenda of 2024
#TOP 1| CVE-2024-3094 XZ Backdoor

What is XZ?

XZ is a general-purpose data compression format used in many Linux distributions. It provides portability by compressing large files into smaller sizes.

What is the CVE-2024-3094 XZ Backdoor Vulnerability and How Does It Work?

This security vulnerability affects various Linux distributions that include XZ Utils versions 5.6.0 and 5.6.1. Distributions such as Fedora 40 and Rawhide, Debian testing and unstable versions, OpenSUSE Tumbleweed, and Arch Linux are particularly affected. The backdoor modifies specific functions in the liblzma library by using a pre-compiled object file (bad-3-corrupt_lzma2.xz) during the build process of XZ Utils. By altering functions in the liblzma library, the backdoor manipulates the behavior of applications that utilize this library.

Exploitation and Effects of the Vulnerability by a Threat Actor:

The CVE-2024-3094 vulnerability allows threat actors to gain persistent access to systems by adding backdoors through the manipulated XZ Utils library, bypass security measures, and steal sensitive data. This vulnerability can be exploited in a wide range of attack scenarios, such as supply chain attacks, APT campaigns, and malware distribution. The manipulated library disrupts application behavior, leading to service interruptions, data manipulation, and weakened system security.

Custom Detection Rules and IoCs Created as ADEO:

The ADEO MDR Service has deployed a total of **2 detection rules** and **63 IoCs** related to the CVE-2024-3094 XZ Backdoor Vulnerability in customer environments.

Top 5 Agenda of 2024
#TOP 2| APT41 Has Arisen From the DUST

APT41 Has Arisen From the DUST:

APT41 is an advanced persistent threat (APT) group conducting targeted cyber espionage attacks on various sectors worldwide. The group employs sophisticated toolsets and techniques to gain prolonged network access and steal sensitive data. Recently, APT41 has targeted organizations in the following sectors:

- Global transportation and logistics
- Media and entertainment
- Technology companies
- Automotive sector

Affected regions include Italy, Spain, Taiwan, Thailand, Turkey, and the United Kingdom.

What Are the Impacts of the Threat Actor?

An advanced threat actor like APT41 can infiltrate target systems using sophisticated toolsets and zero-day vulnerabilities, steal sensitive data, establish long-term persistence, and move laterally within the network to compromise other systems. These attacks can result in serious consequences, including data breaches, operational disruptions, financial losses, reputational damage, and legal penalties.

Custom Detection Rules and IoCs Created as ADEO:

The ADEO MDR Service has deployed a total of **9 detection rules** and **28 IoCs** related to "APT41 Has Arisen From the DUST" in customer environments.

Top 5 Agenda of 2024
#TOP 3| CVE-2024-6387 RegreSSHion Vulnerability

What is OpenSSH?

OpenSSH (Open Secure Shell) is an open-source tool that provides secure remote connections and data transfers. Designed for security, flexibility, and ease of use, OpenSSH is commonly the default protocol on Unix and Linux systems but can also be used on other platforms, including Windows.

What is the CVE-2024-6387 RegreSSHion Vulnerability and How Does It Work?

This vulnerability stems from a flaw in OpenSSH's signal handling mechanism. Signals are used by operating systems to notify processes of specific events. OpenSSH contains a bug that introduces a security vulnerability when handling these signals. If a client fails to authenticate within the LoginGraceTime seconds (default 120, previously 600 in older OpenSSH versions), the sshd's SIGALRM handler is invoked asynchronously, leading to unsafe calls to various asynchronous signal functions.

Custom Detection Rules and IoCs Created as ADEO:

The ADEO MDR Service has deployed a total of **5 detection rules** and **34 IoCs** related to the CVE-2024-6387 RegreSSHion Vulnerability in customer environments.

Top 5 Agenda of 2024

#TOP 4| CVE-2024-38063 Windows IPv6 TCP/IP RCE Vulnerability

What is CVE-2024-38063 Windows IPv6 TCP/IP RCE Vulnerability and How Does It Work?

It is caused by an integer underflow error, especially during the processing of IPv6 packets in Windows. This error allows attackers to trigger a buffer overflow, which enables them to execute arbitrary code on the system.

Attack Vector:

Attackers can exploit this vulnerability by sending specially crafted IPv6 packets to the target system. The attack can be carried out without user interaction, allowing the attacker to execute code with full privileges on the target system.

Custom Detection Rules and IoCs Created by ADEO:

The ADEO MDR Service has transferred a total of **1 detection rule** related to the CVE-2024-38063 IPv6 TCP/IP RCE vulnerability to customer environments.

Top 5 Agenda of 2024
#TOP 5| CVE-2024-49113 LDAPNightmare

What is LDAP?

LDAP (Lightweight Directory Access Protocol) is a protocol used to access directory services over a network. It is commonly used in systems that store information such as user details, groups, and other resources (e.g., Active Directory). LDAP is designed to query and manage information quickly and efficiently.

What is CVE-2024-49113 LDAPNightmare?

CVE-2024-49113 is a critical denial of service (DoS) vulnerability found in the Lightweight Directory Access Protocol (LDAP) service of Microsoft's Windows operating system. This vulnerability allows attackers to send specially crafted LDAP requests, causing the target system to crash and resulting in service disruptions.

How Can an Attacker Exploit This Vulnerability?

An unauthenticated attacker who successfully exploits this vulnerability could gain the ability to execute arbitrary code within the context of the LDAP service. However, successful exploitation depends on which component is targeted.

In the context of exploiting a domain controller for an LDAP server, the attacker would need to send specially crafted RPC calls to trigger a search within the attacker's domain.

In the context of exploiting an LDAP client application, the attacker would need to convince or deceive the victim into querying a domain controller for the attacker's domain or connecting to a malicious LDAP server. However, unauthenticated RPC calls will not succeed.

Impact of the Vulnerability:

The attack flow begins when a DCE/RPC request is sent to the victim server. When the attacker sends a specially crafted Connectionless Lightweight Directory Access Protocol (CLDAP) redirection response packet, it causes the Local Security Authority Subsystem Service (LSASS) to crash and forces a reboot of the system.

Custom Detection Rules and IoCs Created by ADEO:

The ADEO MDR Service has transferred a total of **2 detection rules** related to the CVE-2024-49113 LDAPNightmare vulnerability to customer environments.

Digital Forensics and Incident Response Service

ADEO Digital Forensics and Incident Response Service

Digital Forensics encompasses the processes of obtaining, preserving, and analyzing digital data in accordance with the requirements of evidence collection for presentation in court.

This service involves the collection, preservation, and analysis of digital evidence from systems to uncover the cause of a cyber incident. The digital evidence collected within this service should adhere to the chain of custody principle and be of a quality that can be presented to legal authorities when necessary.

The types of digital evidence and information that can be collected within this service generally include:

- Forensic copies of systems affected by the cyber attack
- Memory images of systems affected by the cyber attack
- Volatile data obtained through live analysis of systems affected by the cyber attack (running applications, open network connections, etc.) or other digital evidence sources required for incident response (event logs, file system records, etc.)
- Raw packet data or network flow data obtained over the network in the event of an ongoing cyber incident

Other types of evidence, such as operating system event logs, file system records, network flow data, etc., which are included in the types of evidence listed above, are examined within the scope of this service when needed during the analysis of cyber incidents. The examination is conducted in forensic computing laboratories containing internationally recognized hardware and software, and by experts holding internationally recognized certifications.

Since 2019, ADEO DFIR team has conducted incident response and security breach detection **on over 400,000 endpoints** for **more than 100 institutions and organizations**, including finance, telecommunications, government agencies, energy, and the private sector.

The entire incident response process is carried out in accordance with internationally recognized incident response plans.

In all cases where intervention is carried out,
- the tactics,
- techniques, and
- tools

used by the attacking group are identified and thoroughly analyzed and reported.

As a result of the Incident Response:

- Access by the relevant attacking group is terminated and blocked from the affected organization.
- A short-term and long-term action plan that needs to be taken is shared with the affected organization.

ADEO Digital Forensics and Incident Response Service

Basic Conditions Observed During Incidents:

Command Injection:
Malicious commands are injected into the system's command line through user inputs, allowing the attacker to perform unauthorized actions. This vulnerability usually arises from unsafe input validation.

Credential Stealing/Accessing Admin Panel of Website:
Unauthorized access to website admin panels is achieved by stealing usernames and passwords. Attacks are typically carried out using keyloggers, phishing, or brute force methods.

Permission Change:
Changing system or file permissions can lead to unauthorized access to sensitive data. This often results from weak user policies or insider threats.

Miner:
The misuse of system resources for cryptocurrency mining. Servers with high processing power are often targeted, leading to a significant decrease in system performance.

Phishing:
Fake emails or websites are used to deceive victims into stealing their credentials or infecting them with malware. It is a popular attack technique that targets the human factor.

RCE (Remote Code Execution):
A critical vulnerability that allows an attacker to remotely execute commands or code. It typically arises from poorly configured applications or outdated software.

Ransomware:
A type of malicious software that encrypts the victim's files and demands a ransom for access. It often spreads through phishing attacks or exploiting security vulnerabilities.

SQL Injection:
By injecting malicious SQL commands into database queries, attackers can retrieve or manipulate data. Weak input validation is the major contributing factor.

USB Malware:
Malware is delivered to systems via physical USB devices. It is commonly used to target offline systems.

Unauthorized Access:
Unauthorized individuals gain access to sensitive documents. This is often caused by weak access controls or insider threats.

Tactics and Techniques Used by Attackers in Observed Incidents:

Obfuscation:
It refers to the tactics and techniques used by attackers to evade detection and avoid triggering alarms from security products by making their actions more complex and confusing. Attackers may encode data and/or add unnecessary code blocks to confuse analysts examining malicious software.

Insider:
This refers to cases where the attacker is someone working within the targeted organization or where attackers collaborate with individuals within the organization to leak sensitive data.

Vulnerability Exploitation:
This refers to the exploitation of current security vulnerabilities and so-called 0-day vulnerabilities. The failure to use security products or keep them regularly updated leads to this situation.

Lateral Movement:
This is the process where attackers use protocols such as SMB, LDAP, and WMI to spread from an initially compromised system to other systems within the environment.

Discovery:
This refers to the reconnaissance performed by attackers either before launching an attack or to propagate within the environment. It includes stages such as identifying target systems and determining individuals to be attacked.

Persistence:
These are the methods used by attackers to maintain a permanent presence on a compromised system. Attackers may aim to establish themselves on structures like Windows services or scheduled tasks.

Tactics and Techniques Used by Attackers in Observed Incidents:

The Most Common Initial Access Methods Used by Attackers in 2024:

Credential Leak:
This is when attackers use previously leaked user data to gain access to a system.

CVE-2023-46604:
CVE-2023-46604 is a deserialization vulnerability in the OpenWire protocol of Apache ActiveMQ. This vulnerability can be exploited by an attacker to execute code on the server where ActiveMQ is running.

CVE-2024-21887 and CVE-2023-46805:
CVE-2023-46805 is an authentication bypass vulnerability that allows an attacker to bypass authentication controls. CVE-2024-21887 is a command injection vulnerability that enables an attacker to impersonate an authenticated administrator and gain remote code execution (RCE) via specially crafted arbitrary commands. Attackers can combine these two vulnerabilities to achieve unauthenticated code execution, leading to data leaks (including user credentials and configuration data), configuration changes, file modifications, webshell deployment, and more.

SQL Injection:
SQL Injection (SQLi) is a type of injection attack that allows the execution of malicious SQL statements. These statements control the database server behind a web application. Attackers can exploit SQL Injection vulnerabilities to bypass security measures in the application.

Spear Phishing:
Spear Phishing is a targeted form of phishing attack aimed at a specific person, group, or organization. These personalized scams deceive victims into disclosing sensitive data, downloading malware, or sending money to an attacker.

Insider:
This refers to situations where the attacker works within the targeted organization or collaborates with employees inside the organization to leak data from within.

Tactics and Techniques Used by Attackers in Observed Incidents:

Attackers' Money-Making Methods:

Ransomware:
An attack where attackers encrypt critical data on a server and extort the victim for the decryption key in exchange for a ransom.

Miner:
An attack where attackers exploit server resources to mine cryptocurrencies such as BTC, ETH, XMR, for their own profit.

Data Theft:
An attack where attackers steal data from the server and then sell it on underground forums.

Blackmailing:
An attack where attackers threaten to disrupt the victim's services and extort money from the organization owners to avoid service interruption.

Most Commonly Encountered APT Groups in 2024:

In the research conducted by the ADEO DFIR team in 2024, various APT groups were encountered. It was determined that the general motivation of these APT groups was to carry out ransomware attacks.

The related APT groups are as follows:

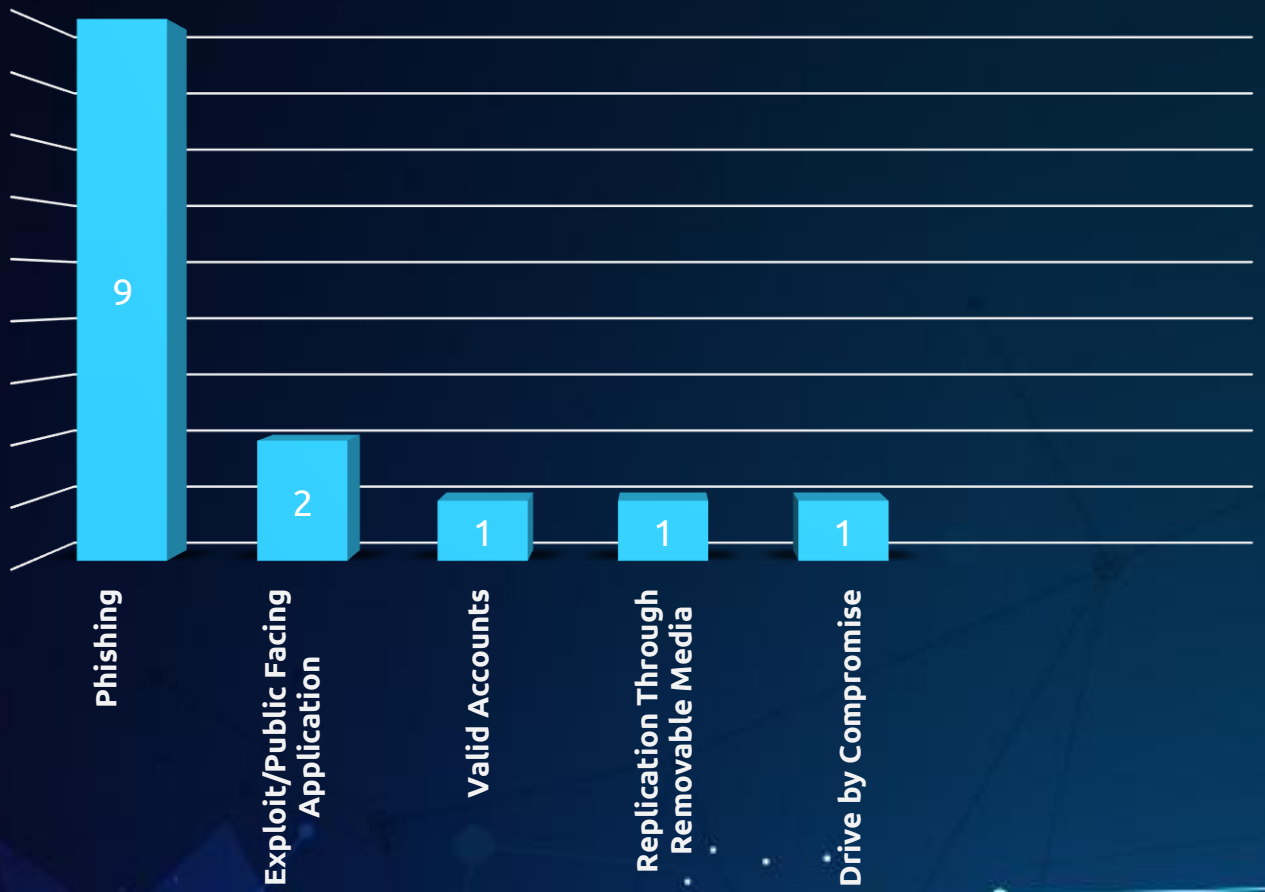
- Lockbit Ransomware
- Conti Ransomware
- SeXi APT Inc Ransomware
- Mimic (N3ww4v3)
- Phalcon Ransomware

Sectors Most Targeted by APT Groups in 2024:

- Banking and Finance
- Manufacturing
- IT Services
- Education
- Healthcare
- Tourism
- Aviation
- Non-Profit Organizations

ADEO MDR Service
Tactics, Techniques and Detection Rules

Most Used Initial Access Technique



An attacker's ability to gain a foothold in the environment **begins with initial access.**

The credentials of compromised accounts can be compromised by various techniques and used to bypass access controls applied to different resources on systems within the network.

After initial access, the attacker can switch to other tactics and techniques to achieve objectives.

Therefore, preventing the first access is important for the security of the system.

ADEO's Attack Detection Rules

Cyber Security Peak: ADEO's 96% Success!

Cyber attacks are increasing and becoming more sophisticated day by day. Therefore, investing in cybersecurity and proactively protecting against threats is more crucial than ever.

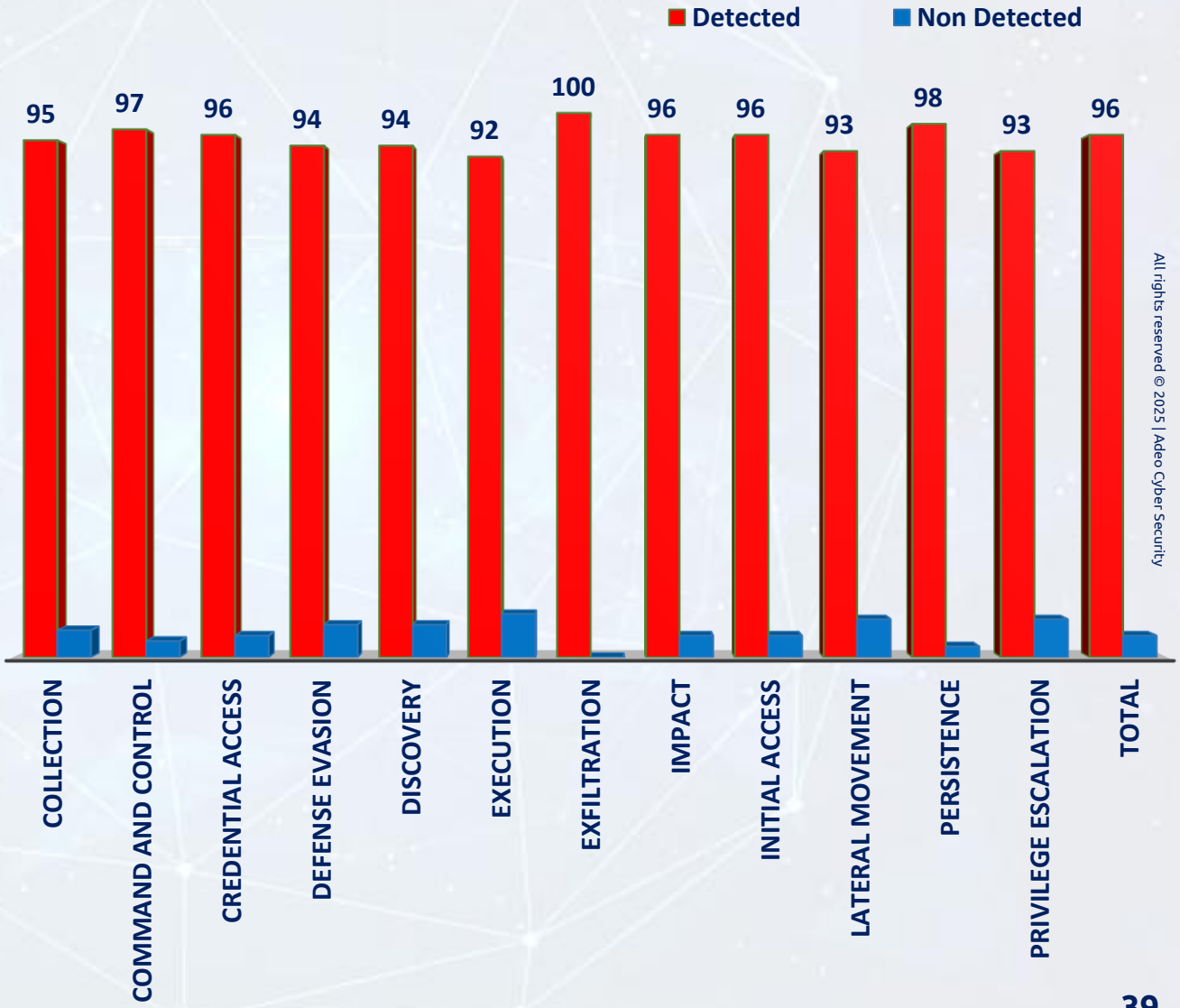
As ADEO, we use
- the latest technology and
- the expertise of the most competent analysts

in our cybersecurity approach to protect our customers against cyber attacks.

Our service, **with a detection rate of 96%,** stands as a concrete demonstration of our expertise in the 2024 report.

After 2592 actions in 2024, with reference to 12 MITRE ATT&CK TTP values, it is observed that **we have an average detection rate of 96%.**

Despite the increase in MITRE ATT&CK TTP numbers over the past three years, our active rule development efforts have enabled us to maintain this rate **above 96%.**



1.Collection

The adversary is trying to gather data of interest to their goal.
Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives.
Frequently, the next goal after collecting data is to steal (exfiltrate) the data. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.

95% of the attacks made using the Collection tactic can be detected by our ADEO MDR Service.

In addition to EDR technology, it is recommended to implement data loss prevention systems for the detection of these and similar attacks. It is recommended to use **DLP technology**, which is an additional data leakage prevention system, for studies such as planning controls such as reducing the risk, impact and degree of attack and ensuring the continuity of policies.

XDR, NDR, Firewall, DLP technologies are recommended to prevent the leak attempts of **compressed or encrypted** files and to perform user behavior analysis (UBA).

It is important to organize **awareness trainings** at regular intervals in order to increase user awareness.

It is recommended to keep **the system images and software used up-to-date.**

In an **Exchange environment, Exchange rules** need to be tightened to prevent administrators from doing potentially malicious automatic forwarding, downloading, and opening.
Using multi-factor authentication (MFA) for externally accessible e-mail servers will greatly reduce attacks.

%95

2.Command And Control

The adversary is trying to communicate with compromised systems to control them.
Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection.
There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

97% of the attacks made using the Command and Control tactic can be detected by our ADEO MDR Service.

Web traffic to/from known **bad or suspicious domains should be monitored.**

It is recommended **to filter DNS requests** to unknown, untrusted or known bad domains and resources through the **firewall.**

It is recommended to use **Firewall, NDR, IDS/IPS in addition to EDR** for the detection of these and similar attacks and **UBA-based products** for user behavior analysis.

It is necessary to **monitor the traffic** in the network and to **constantly check the IP's going from inside to outside and coming from outside with intelligence services.**

Applications that can be installed on the system must pass through the approval mechanism and must be in the list of allowed applications (**White List).** Your computer system should not allow any application to be run or installed. **By blocking the installation** of applications from unknown sources, **you can prevent malware** used to create C2 channels from being installed on your system.

%97

3.Credential Access

The adversary is trying to steal account names and passwords.
Credential Access consists of techniques for stealing credentials like account names and passwords.

Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

96% of the attacks made using the Credential Access tactic can be detected by our ADEO MDR Service.

WAF is a common security control used by organizations to protect web systems from zero-day exploits, remote command execution, and other known and unknown threats and vulnerabilities.

It is recommended to **locate WAF within the organization.**

Passwords should not be used on different platforms, the password should be considered for a **maximum of 1 or 3 months**, and it should be considered to have special features. It is **important to avoid unnecessary/over-authorization**, and to close the existing accounts after the staff leaves the job. **File shares** should be **limited to specific directories** that only have access to required users.

It is recommended to place **Privileged Access Management (PAM**) products within the organization in order to securely manage the accounts of users with access permissions to critical resources.

It is important **to activate MFA** in all possible logins, especially VPN and E-mail access.

It is important to isolate the departments from each other **by using VLAN** and to minimize the possible dangers.

It is recommended to regularly update **the security updates** of the applications where **the credentials are hosted**, especially the Domain Controller servers.

%96

4. Defense Evasion

The adversary is trying to avoid being detected. Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise.

Techniques used for defense evasion include uninstalling/ disabling security software or obfuscating/encrypting data and scripts.

Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

94% of the attacks made using the Defense Evasion tactic can be detected by our ADEO MDR Service.

It is recommended to save/archive the logs of the relevant applications in a central point in order to analyze the activities performed via **PowerShell** and **Command Prompt** command line applications. It is recommended to position **Load Balance**, **DDoS Protection** products in-house to protect against denial of service attacks (**DoS/DDoS**) and to minimize attack types.

It is recommended to **limit user privileges**. Only authorized users should be limited to making service changes. It is recommended to **prevent execution** from user directories such as file download directories and temporary files directories.

Attackers can abuse compiled **HTML files (.chm)** to hide malicious code. CHM files are often distributed as part of the Microsoft HTML help system. CHM files are compressed compilations of various content such as **VBA, JScript, Java and ActiveX. With application whitelist software, the execution of such uncommon script extensions can be prevented or detected.**

It is recommended **to disable/remove** the security vulnerabilities of applications that are **not needed in-house.** In order to prevent **phishing** attacks via e-mail, it is important to position **Sandbox-derived** technologies and **Email Security Gateway** products, and to make security updates of used **application inventories** at regular intervals.

%94

5.Discovery

The adversary is trying to figure out your environment.

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

94% of the attacks made using the Discovery tactic can be detected by our ADEO MDR Service.

The existing environment in the institutions (**with the help of Active Directory, Firewall, Network Segmentation** and other security devices, if any) should be tightened in accordance with the needs and **the attack surface should be narrowed.** It is recommended to tighten and mature the **Audit** and **Log levels** running on the environments.

In order to prevent the risk of discovery and possible exploitation, asset inventories should be examined periodically, making sure that **unnecessary ports, and services are closed**. It is recommended to **use IPS/IDS technologies** to detect and prevent remote service scans.

Many important information is also available through Windows Management Instrumentation and Windows system management tools such as PowerShell. **Windows event logs** must be configured and collected centrally to identify such actions that can be taken to gather system and network information.

Security updates of applications in asset inventory should be checked periodically.

User account management should be provided, and the **least privilege policy** should be applied.

%94

6.Execution

The adversary is trying to run malicious code.

Execution consists of techniques that result in adversary-controlled code running on a local or remote system.
Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

92% of the attacks made using the Execution tactic can be detected by our ADEO MDR Service.

By opening a malicious file or link, the user can be subjected to a social engineering attack to execute malicious code. In order to prevent such attacks, it is necessary to **regularly check and update the e-mail or internet browser applications** on the end user's side.

Visibility on network traffic should be increased with NGFW or NDR products to prevent or detect attackers from **exploiting RCE vulnerability**.

The existing environment in the institutions **(with the help of Active Directory, Firewall, Network Segmentation and other security devices, if any)** should be tightened in accordance with the needs and the **attack surface** should be narrowed. It is recommended to tighten and mature the **Audit** and **Log** levels working on the environments and to use **SIEM** technologies.

Any **RCE vulnerability** that can be found on **open servers** will allow the attacker to easily enter the corporate network. With the **Zero Trust** security strategy, **access from external servers** to internal or other servers should **be limited and monitored by network access control (NAC) tools.**

%92

7.Exfiltration

The adversary is trying to steal data.

Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption.
Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission.

100% of the attacks made using the Exfiltration tactic can be detected by our ADEO MDR Service.

For data to leave the network, it must pass through a designed exit point. **A next-generation firewall (NGFW)** with signature-based antivirus features typically useful for C2 detection **can help detect or prevent an infiltration. A network intrusion prevention system (IPS)** that can see traffic protocols **can help detect and prevent leakage.**

DLP monitors the unauthorized access and use of sensitive data by the user. It is recommended to use it as it **prevents data from coming out.**

Attackers spread over the network by running malicious code **over USB.** In some cases, **data hijacking can occur via a user-identified USB device.** The USB device can be used as the last data evasion point or otherwise to switch between disconnected systems. In order to prevent this, it is recommended to **disable the usb ports in low awareness areas.**

Instead of sending data in one piece, an attacker can **send files in pieces.** In this way, it ensures the transmission of data without exceeding the minimum upload size.
Continuous monitoring of network traffic is recommended to prevent an attack.

%100

8.Impact

The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.

Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

96% of the attacks made using Impact tactic can be detected by our ADEO MDR Service.

Ransomware can encrypt data on target systems or multiple systems in a network **to cut off** access to system and network resources. In order to prevent attacks, it is recommended **to prepare backups** by preparing **disaster scenarios** and make these backups inaccessible to attackers.

A denial of service attack results in a successful **DDoS attack** when the attacked resource is exposed to requests from multiple machines and does not respond by exceeding its capacity. **To prevent DDOS**, it is recommended **to filter traffic and take DDoS prevention service provided by Content Delivery Networks (CDN) or providers specializing in DoS mitigation.**

Data Manipulation: Attackers can add or delete data, hiding their activities with different results. In this way, they may try to influence a business process, organizational understanding, or decision-making by manipulating their competitor's data. It is recommended to **use data encryption, storage method and DLP solutions to prevent financial losses that may occur.**

Man in the Middle attack is an attack method that takes place in the form of interception of various data by listening to the communication between two connections in the network or manipulating the data by listening to the communication and creating a misleading communication. In order to prevent MitM attack types, it is important to **use SSH, IPSec protocols, HTTPS supported sites, and not to connect to unencrypted WIFI networks shared in public environments.**

%96

9.Persistence

The adversary is trying to maintain their foothold.

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

98% of the attacks made using the Persistence tactic can be detected by our ADEO MDR Service.

NDR gives you transparency on all connections and protocols. It deeply scans traffic and performs retrospective analysis to analyze connections, streams, packets and metadata in real time. **To minimize the resolution time of a detected threat,** it is recommended to **use an integrated network detection and response solution.**

Prevention: It is important to have **a weekly malware scan** for all devices on the network. In addition, security breach analysis and evaluation (Compromise Assessment) studies should be carried out **at regular intervals.**

By running **remote commands** on assets that contain various vulnerabilities, system shutdown/restart, attackers can cause data corruption, material damage and loss of life in environments and places such as e-commerce and hospitals. It is recommended to use **Extended Detection and Response (XDR), Firewall, Backup technologies** to prevent these and similar types of attacks.

Downloads such as **fake/cracked** programs, games, operating systems can make your system the target of serious attacks. It may expose institutions to attacks such as ransom, data breach, and backdoor. These and similar attacks are usually **caused by low user awareness**. For this reason, it is recommended to **give basic safety training to employees at regular intervals.**

%98

10.Privilege Escalation

The adversary is trying to gain higher-level permissions.
Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.
Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

Examples of elevated access include:
- SYSTEM/root level
- Local administrator
- User account with admin-like access
- User accounts with access to specific system or perform specific function.

These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.

93% of the attacks made using the Privilege Escalation tactic can be detected by our ADEO MDR Service.

Logs from directory servers such as **Active Directory (AD)** or **LDAP** need to be configured. User rights upgrade or new user creation events need to be followed. It is necessary to create a list of privileged user account names, authorizations. Privilege Escalation attacks or attacks against privileged users can be detected using Identity-based Security products.

Privileged access rights need to be reviewed at appropriate intervals (at least once a month) and the assignment of **privileged permissions should be reviewed regularly**. All privileged access to files and databases (including local system access) **must be monitored.** The alarm mechanisms of critical privileged user changes should be instantly shared with the relevant IT managers by creating Mail-SMS.

Make sure that users have **directory access control set up** to reduce places where malicious files can be placed for execution. It is recommended that all executables be **placed in write protected directories.**

It is important to detect security vulnerabilities before attackers take advantage of these vulnerabilities. **An effective scanning process with vulnerability scanning tools;** reveals system **misconfigurations, weak passwords, and weaknesses in Web Server Security.**

For keeping threat vectors away from institutions with effective vulnerability scanning it is **important to update**, patch or deploy additional layers of security.

%93

11.Initial Access

The adversary is trying to get into your network.

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network.

Techniques used to gain a foothold include targeted spear phishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

96% of the attacks made using the Initial Access tactic can be detected by our ADEO MDR Service.

It is important for users **not to use their passwords on social networks and other platforms** when setting a password. The change interval of passwords should be between **1 and 3 months**. It must contain special characters and have a **minimum of 14 characters.**

Unnecessary authorization should be avoided during **account authorization**. It is important to close the accounts of the dismissed employee.

URL analysis (including expanding shortened links) within the email can help detect links to known malicious sites.

Sandbox solutions can be used to detect these links and detect malicious behavior by automatically accessing these sites or to wait and capture content if a user visits the link.

It is necessary to collect **authentication logs** and detect unusual / unauthorized access outside of normal working hours.

It is important to **update the used application asset inventories** (web browsers, components, plug-ins, office and media etc.) **on a regular basis.**

Network traffic classified as malicious by threat intelligence sources **should be blocked and alerts should be created.**

%96

12.Lateral Movement

The adversary is trying to move through your environment.

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it.
Reaching their objective often involves pivoting through multiple systems and accounts to gain.
Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

93% of the attacks made using the Lateral Movement tactic can be detected by our ADEO MDR Service..

Lateral movement techniques may be legitimate **depending on the network environment** and how they are used. Factors such as files accessed or activities occurring after a **remote desktop protocol (RDP)** may indicate suspicious or malicious behavior associated with this activity. It is recommended to **monitor user accounts logged into systems** that would normally not be able to access multiple systems in a relatively short time.

By isolating VLAN networks from each other, it prevents the spread of attacks and data breaches.

Restricting the systems or services accessed by **VPN** will keep the internal spread to a minimum in case VPN accounts are compromised.

If the use of **WinRM** is not common by system teams, it should be disabled. If widely used, Windows event logs should be configured and centrally collected on **SIEM**.

Suspicious accesses should be detected through these logs collected with the written rules.

The use of **SSH** may be legitimate depending on the network environment and how it is used. Other factors, such as activity after remote login, may indicate suspicious or malicious behavior. It is necessary to **monitor user accounts logged into systems** that would normally not be able to access multiple systems in a relatively short time.

%93

Rule Distribution by Operating Systems

As ADEO MDR Service, we have a total of **5500+** detection rules tailored for Windows, Linux, MacOS operating systems, and their derivatives (such as Windows Server, Workstation, CentOS, Unix, Debian, Ubuntu-based, etc.).

The distribution of developed detection rules is as follows: **4808 for Windows operating system, 717 for Linux,** and **755 for MacOS.**

The detection rules we have developed cover approximately **96%** of the Tactics, Techniques, and Procedures (TTPs*) in the MITRE ATT&CK® Framework for all operating systems based on Linux, MacOS, and Windows.

This enables us to provide support with a detection rate of **over 96%** for all our customers across three operating systems and their derivatives.

TTP
An abbreviation for Techniques, Tactics and Procedures used to describe/describe the operation of a threat actor. TTPs are used to profile a specific threat actor.

We provide support with a detection rate of over 96% for three operating systems and their derivatives for all our customers.

4808

755

717

2025 Cyber Security Trends and Predictions

2025 Cyber Security Trends and Predictions

1. Artificial Intelligence: The New Frontier of Threats and Defense

Artificial intelligence is at the heart of cybersecurity in 2025. While 66% of organizations predict AI will have a major impact on cybersecurity, 47% are seriously concerned about threats stemming from generative AI. Threat actors are leveraging AI to create enhanced malware that evades antivirus solutions and using deepfake technology to conduct social engineering attacks. On the defense side, AI is providing critical tools for autonomous threat detection and rapid response, boosting the efficiency of SOC teams.

From a defense strategy perspective, AI offers significant advantages in anomaly detection, alert prioritization, and automating routine tasks. However, as this technology is susceptible to counterattacks such as data poisoning, ensuring the security of AI systems and monitoring their decisions is becoming increasingly important.

2. Ransomware and Supply Chain: Evolving Attack Vectors

Ransomware attacks are evolving in 2025, adopting a "double extortion" tactic that combines data encryption with the threat of data leaks. With global costs expected to reach $30 billion, this threat particularly targets sectors with low tolerance for disruptions, such as healthcare, education, and public services. Supply chain attacks are also emerging as a major threat vector, with 54% of large companies citing supply chain dependencies as the biggest obstacle to their cyber resilience.

Attackers exploit weaker suppliers as entry points to reach organizations that are harder to target directly. Techniques such as "update poisoning" and the takeover of supplier accounts enable a single compromised software library to impact thousands of applications, posing a significant risk.

2025 Cyber Security Trends and Predictions

3. IoT and Operational Technology Security

A 400% increase in attacks targeting IoT devices over the past year highlights the growing importance of this area. The fact that 98% of IoT traffic is transmitted unencrypted and that most devices run outdated operating systems creates significant risks, especially in manufacturing, energy, and healthcare sectors. Compromised IoT devices can be used to form botnets for large-scale DDoS attacks.

Operational technology (OT) systems are becoming a national security concern as part of critical infrastructure. In 2025, more countries will implement dedicated cybersecurity standards for power grids, water distribution systems, and manufacturing facilities. Regulations such as the EU's Cyber Resilience Act are preparing to enforce minimum security requirements for IoT device manufacturers.

4. Enterprise Defense Strategies and Technologies

Zero Trust architecture is becoming the foundation of corporate defense strategies in 2025. With 60% of large enterprises expected to adopt this security framework, identity and access management-focused approaches are continuously verifying every access request to limit unauthorized lateral movement. Cyber resilience is also gaining prominence; organizations are not only focusing on preventing attacks but also on strategies to recover quickly when an attack occurs.

The trend of security tool consolidation is strengthening, with organizations shifting from using numerous separate security tools to integrated platforms. SOAR (Security Orchestration, Automation, and Response) systems and AI-driven threat hunting practices are becoming widespread, while preparations for post-quantum cryptography are underway to address the threat posed by quantum computing. Cybersecurity literacy among board members is increasing, with nearly half of CISOs now reporting directly to the CEO.

2025 Cyber Security Trends and Predictions

5. Regulatory Landscape and Global Collaboration

Cybersecurity regulations will become even stricter on a global scale in 2025. In the U.S., the SEC mandates that publicly traded companies disclose major cybersecurity incidents within four business days. In the EU, the NIS2 Directive expands cybersecurity requirements and incident reporting obligations across a broader range of sectors, while the AI Act classifies AI systems based on risk levels, imposing new responsibilities on companies.

The variation in regulations across countries creates challenges for multinational companies, with 76% of cybersecurity leaders stating that this fragmented landscape complicates compliance efforts. However, public-private sector collaboration and regional initiatives are strengthening. Structures like NATO cyber exercises, ASEAN initiatives, and regional CERT networks facilitate information sharing. The World Economic Forum emphasizes that the digital world can only remain secure through close cooperation between the public and private sectors.

The variation in regulations across countries creates challenges for multinational companies, with 76% of cybersecurity leaders stating that this fragmented landscape complicates compliance efforts. However, public-private sector collaboration and regional initiatives are strengthening. Structures like NATO cyber exercises, ASEAN initiatives, and regional CERT networks facilitate information sharing. The World Economic Forum emphasizes that the digital world can only remain secure through close cooperation between the public and private sectors.

2025 Cyber Security Trends and Predictions

Recommendations:

- **Adopting and Controlling AI:** Organizations should experiment with AI-based security solutions but should not view them as a silver bullet. AI-powered anomaly detection tools can be highly beneficial for network security, but their outputs should always be verified by experts.
- **Ensuring Basic Cyber Hygiene:** Fundamental measures such as strong password policies, multi-factor authentication, regular patching of systems and applications, data backups, and network segmentation can prevent many attacks.
- **Updating Incident Response Plans:** Clearly defining roles, communication flows, and regularly testing incident response (IR) plans is critical. To be fully prepared for potential cyberattacks in 2025, ensure that your IR plans are up-to-date, well-communicated, and followed by all teams and stakeholders.
- **Taking a Proactive and Intelligence-Driven Approach:** Acknowledging that attacks are inevitable, organizations should focus on the "when" rather than "if" and remain vigilant. Leveraging threat intelligence services to stay updated on the latest attack techniques and targeted industries is now more critical than ever.
- **Investing in the Human Factor:** It is widely recognized that people managing and using technology are just as crucial as the technology itself. Enhance your cyber resilience through phishing simulations, regular security training, and cyber crisis management workshops—especially for senior executives.

While 2025 presents significant cybersecurity challenges, it is also a year of innovation and transformation. Attackers may be more sophisticated and faster than ever, but as long as the defense side does its part, there is no need to fear.

VP of Global Strategy
Halil Öztürkci

Cybersecurity Strategies in the Age of Artificial Intelligence

Cybersecurity Strategies in the Age of Artificial Intelligence:

Building Corporate Resilience:

With the widespread adoption of information technologies and the acceleration of digital transformation, cybersecurity has become one of the most critical strategic challenges faced by modern institutions. Going beyond traditional threat vectors, sophisticated elements such as AI-powered attacks, advanced persistent threats (APTs), supply chain vulnerabilities, and deep learning-based manipulations further deepen the fragility of our digital ecosystem. In this context, it is imperative for institutions and organizations to restructure their cybersecurity approaches within a long-term strategic vision rather than focusing solely on tactical defense mechanisms. This article will analyze the fundamental components of cybersecurity strategies for 2025 and beyond from an academic perspective and present a comprehensive plan for building corporate resilience.

The Strategic Imperative of Cybersecurity: Multi-Layered Risk Management:

Today, cyber threats have evolved beyond being merely a technical issue under the responsibility of IT departments, becoming a risk factor with strategic implications across a broad spectrum, including corporate sustainability, reputation management, financial stability, and even national security. Cyberattacks can cause operational disruptions, data breaches, loss of intellectual property, and legal sanctions, posing significant threats to an organization's core functions and long-term objectives. Therefore, cybersecurity must be integrated as an essential component of the corporate risk management framework and positioned as a strategic priority at the executive level.

From Tactical Defense to Strategic Resilience: An Integrated Framework:

An effective cybersecurity strategy must go beyond reactive measures and be built on an integrated framework that includes proactive defense, early detection, rapid response, and efficient recovery processes. In this context, the concept of "strategic resilience" comes to the forefront. Strategic resilience refers to an organization's ability not only to defend against cyberattacks but also to ensure business continuity, resume operations in the shortest possible time, and maintain its competitive advantage in the long run. To achieve this goal, organizations must develop a comprehensive cybersecurity strategy and integrate it into all business processes.

Cybersecurity Strategies in the Age of Artificial Intelligence:

Advanced Persistent Threats (APTs) and State-Sponsored Actors: A Complex Threat Landscape:

One of the most critical components of strategic cyberattacks is advanced persistent threats (APTs) and state-sponsored actors. These attacks typically require a high level of technical expertise, patience, and resources. The primary objective is to infiltrate a system covertly, maintain a presence for an extended period, and gain access to sensitive information.
The XZ Utils attack discovered in 2024 serves as a striking example of how complex and stealthy such threats can be. This sophisticated attack targeted an open-source software component and had the potential to impact numerous systems globally. It is believed to have been carried out by a state-sponsored actor. This incident underscores the necessity for organizations to remain vigilant not only against external threats but also against potential vulnerabilities within their supply chains and open-source projects.

Formulating a Proactive Threat Intelligence Strategy:

The foundation of an effective cybersecurity strategy lies in a proactive threat intelligence approach. This approach goes beyond merely tracking known threats and attack methods; it also involves understanding potential attackers' motivations, objectives, and tactics. Advanced threat intelligence platforms, dark web analyses, industry information-sharing networks, and academic research serve as key sources of information in this context. By analyzing data from these sources, organizations can gain a deeper understanding of their specific threat landscape and tailor their defense mechanisms accordingly. Integrating threat intelligence into strategic decision-making processes plays a crucial role in developing long-term security plans.

Addressing Systemic Vulnerabilities: The Open-Source Software Example

The widespread use of open-source software (OSS) brings significant security risks. Vulnerabilities in OSS projects can be exploited by malicious actors for large-scale attacks, making it essential for organizations to adopt a strategic approach to OSS usage. This approach should include maintaining an inventory of OSS components, conducting regular vulnerability scans, strengthening patch management processes, and prioritizing reliable OSS sources. Additionally, contributing to the security of OSS projects and collaborating with the community can serve as a strategic step toward enhancing long-term security.

Cybersecurity Strategies in the Age of Artificial Intelligence:

Cybercrime-as-a-Service (CaaS) Ecosystem: A Strategic Challenge

The Cybercrime-as-a-Service (CaaS) model has significantly increased the scale and complexity of cyberattacks. Attackers can purchase various cybercrime services, from ransomware operations to phishing campaigns, from specialized groups. This reality necessitates that organizations develop a multi-layered defense strategy and strengthen their incident response capabilities. At a strategic level, enhancing national and international cooperation against such threats is crucial for identifying, apprehending, and prosecuting cybercriminals.

Strategic Implications of Legal Regulations: NIS2 and Beyond

Legal regulations in cybersecurity significantly influence organizations' strategic decisions. Regulations such as the EU's NIS2 Directive establish cybersecurity standards and compliance requirements for organizations operating in critical sectors. Ensuring compliance with such regulations not only helps organizations meet legal obligations but also enhances their cyber resilience and strengthens stakeholder trust. At a strategic level, organizations must closely monitor these regulations, plan their compliance processes, and make necessary investments to stay ahead of evolving requirements.

Protecting Intangible Assets: Brand Security in the Digital Age

Brand security is one of the most valuable intangible assets for organizations today. Cyberattacks and digital fraud activities can severely damage brand reputation and undermine customer trust. Therefore, safeguarding brand security must be a strategic priority for organizations. In this context, implementing measures such as domain management, brand monitoring systems, social media security, and customer awareness initiatives is crucial. At a strategic level, brand security should be integrated with corporate communication and marketing strategies to ensure a comprehensive approach.

Cybersecurity Strategies in the Age of Artificial Intelligence:

Key Strategic Elements of a Future-Oriented Cybersecurity Strategy:

To develop a long-term cybersecurity strategy against an evolving threat landscape, it is essential to focus on the following key strategic elements:

- **Zero-Trust Architecture:** In today's world, where traditional perimeter security models are insufficient, a zero-trust architecture provides a more secure approach by requiring authentication and authorization for all users and devices. Strategically adopting this architecture can enhance resilience against both internal and external threats.
- **Security by Design Principle:** Considering security requirements from the early stages of software and system development helps identify and address potential vulnerabilities before they become costly issues. Strategically implementing this principle contributes to the development of more secure systems in the long run.
- **Continuous Improvement and Adaptation:** Since the cyber threat landscape is constantly evolving, cybersecurity strategies must be dynamic and adaptive. Regular security assessments, keeping threat intelligence up to date, and adjusting strategies to address emerging threats form the foundation of the continuous improvement principle.

Developing a Security-Focused Culture: The Human Factor in Strategic Defense

The human factor plays a critical role in the success of a cybersecurity strategy. Educating and informing employees about cybersecurity can significantly impact an organization's overall security posture. At a strategic level, organizations must develop a long-term plan to foster a security-focused culture. This plan should include regular awareness training, phishing simulations, and an environment that encourages compliance with security policies.

Conclusion: Strategic Agility in the Era of AI-Powered Threats

The period beyond 2025 will witness the increasing prevalence and sophistication of AI-powered cyber threats. To succeed in this challenging environment, organizations must move beyond traditional defense approaches and adopt a comprehensive cybersecurity strategy that incorporates strategic agility, proactive threat intelligence, zero-trust architecture, security by design principles, and a security-focused culture.

It is essential to recognize that cybersecurity is not merely a technological investment but a strategic imperative that underpins corporate sustainability and long-term success. Therefore, organizations must prioritize cybersecurity and remain prepared for the ever-evolving threat landscape.

Melih Özhan
Chief Strategy Officer

Recommendations

Recommendations #TOP5

1

In order to prevent a possible attack, the institution must be monitored 7x24x365 days with the MSSP or MDR service.

2

It is important to activate dual authentication MFA, avoid unnecessary authorization, and take preventive measures in places where awareness is low.

3

In order to increase detection capabilities, it is primarily important to increase visibility. The rules and correlations that will detect the relevant attacks must be constantly updated.

4

Despite possible cyber incidents, an up-to-date action plan should be created and the simulations should be repeated periodically to keep awareness and preparations up-to-date.

5

It is necessary to examine the asset inventories at certain periods and provide the control of outsourced services.

Recommendations

It is important to fully monitor the visibility and tightening of all IT and OT systems.

Rather than purchasing automated products and software, systems, human-based services or investments in people in cyber security teams need to be increased.

It should be ensured that the Red Team and Penetration Test activities are carried out by expert teams at regular intervals.

It should be kept in mind that most of the attacks are caused by newly discovered vulnerabilities. Starting from here, it is important that the "Vulnerability Management" procedures are applied continuously and that they are strictly followed.

Giving practical awareness training to users and employees against phishing attacks at certain intervals is beneficial in preventing human-induced attacks.

It should be ensured that the Purple Team actions for measuring the maturity level of cyber security teams are taken by expert teams.

The existing environment in the institutions (Active Directory, Firewall, Network Segmentation and other security devices, if any) should be tightened in accordance with the needs and the attack surface should be narrowed.

Since 2023,
ADEO has been using various AI models, including ChatGPT.

Artificial Intelligence and Cybersecurity: The Defense Strategy of the Future

In today's rapidly digitizing world, cybersecurity has become vital for organizations. With technology constantly evolving, cyber attacks are becoming increasingly sophisticated. At this point, artificial intelligence (AI) technologies have become one of the most powerful defense mechanisms in the hands of cybersecurity experts.

As a cybersecurity company, we as ADEO go beyond traditional methods by actively utilizing artificial intelligence and machine learning technologies. These technologies assist us in protecting sensitive data and detecting and preventing attacks, as well as gaining different perspectives.

Our Areas of Expertise: Defense Shields and Transition to Automation:

Our areas of operation are focused on enhancing security by developing advanced defense strategies for both our clients and our own company. We utilize this approach to better analyze attacker perspectives and to optimize our rules, while also integrating AI-assisted automation technology to use human resources more efficiently as ADEO.

In the coming years, we plan to actively utilize artificial intelligence in various areas such as alarm analysis, rule writing, and current intelligence gathering, with a rate exceeding 70%.

It is important to emphasize that artificial intelligence technologies will shape the future of cybersecurity. AI systems that can continuously analyze data, learn, and improve themselves will play a critical role in preventing cyberattacks and minimizing their impact.

As ADEO, we are prepared to provide our clients with this new technology, which is vital for their operations. We understand the importance of cybersecurity in today's digital world, and we strive to offer the best service to our clients by utilizing the latest technologies such as artificial intelligence in this field.

New Members of Product Family

Smart Security and Rapid Threat Detection with Splunk SIEM

Splunk SIEM quickly detects security threats with advanced data analytics and AI support. It provides robust protection against cyberattacks through real-time analysis and a powerful correlation engine. Splunk SIEM centralizes, monitors, and reports security data on a single platform.

API Security and Bot Management with Cequence

Cequence offers powerful solutions for API discovery, security, and bot management. It protects your digital assets with AI-powered threat detection, real-time API monitoring, and advanced fraud prevention. Cequence ensures API security, supports regulatory compliance, and reduces organizational risks. With flexible deployment options, it provides solutions tailored to every industry.

Make Your API and Web Applications More Secure with Wallarm

Enhance the security of your API and web applications with real-time protection and automated security tests against OWASP Top 10, bot attacks, and L7 DDoS threats using Wallarm.

Proactive Security and Threat Detection with IBM QRadar

IBM QRadar quickly detects security threats with its advanced correlation engine and AI support. It provides robust protection against cyberattacks through real-time analysis and automated features. With centralized data collection and visualization tools, you can easily monitor your security status.

New Members of Product Family

Zero Trust and Advanced Security Solutions with SecHard

SecHard quickly detects and neutralizes digital risks with AI-powered threat detection, forensic analysis, and security analytics. It provides proactive protection for organizations through real-time threat monitoring and risk assessment. Adopting the Zero Trust approach, SecHard ensures the security of all your assets.

Digital Risk Protection and Proactive Threat Management with Brandefense

Brandefense offers AI-powered digital risk protection and cyber threat monitoring solutions. It provides real-time threat tracking, brand protection, and preventive security services against cyberattacks. The platform detects, prioritizes, and safeguards organizations from potential threats across the deep, surface, and dark web layers.

Proactive Solution with Soteryan AI-Powered Advanced Threat Intelligence

Soteryan provides advanced threat intelligence and security solutions for leading organizations in the cybersecurity field. With AI-powered threat hunting, it effectively neutralizes digital risks, strengthening your organization's security. Real-time threat monitoring, comprehensive data analytics, and prioritized threat reporting enable rapid response to potential attacks. Additionally, by tracking billions of active infection records, it delivers localized analysis of global threats and proactively reports evolving cyber risks. Soteryan enhances organizations' security levels through forensic analysis, security analytics, and risk assessments, safeguarding them against cyber threats.

Advanced Active Directory Security and Threat Management with Forestall

Forestall provides comprehensive solutions for Active Directory security. FSProtect detects misconfigurations and hidden attack paths, while FSDetect ensures continuous monitoring and threat detection. Additionally, Borabay analyzes malicious macros and RTF vulnerabilities in office documents to secure your data. With robust threat detection and a rapid, solution-oriented approach, Forestall protects your organization against advanced threats.

New Members of Product Family

Advanced Asset Management and Security Monitoring with OctoXLabs

OctoXLabs enables centralized management of all cyber assets through its Cyber Asset Attack Surface Management (CAASM) platform. With API integrations, it enhances security by discovering assets, detecting vulnerabilities, and mapping risks. Additionally, it optimizes cybersecurity processes with application inventory and license management.

Fast and Effective Incident Response with Phishy

Phishy provides advanced incident response solutions for email security. It quickly detects and analyzes suspicious emails, determining whether threats are real or fake. With in-depth email analysis, threats can be isolated company-wide with a single click. Additionally, its automated email removal feature helps keep the network secure.

Service Network

Firsts in ADEO and in Turkey

You can explore ADEO Cyber Security's exclusive cybersecurity services on our website www.adeosecurity.com and access the

MSSP Alert Top 250 2024 List via the link below.

Firsts in ADEO and in Turkey

Microsoft MISA Member

First Microsoft MISA Member (2022)

Microsoft MSSP Partner

First Microsoft MSSP Partner (2022)
(It is ranked 2nd in the region and 8th globally.)

ADEO is the first and only Cyber Security company in Turkey to be admitted to the Microsoft Intelligent Security Association (MISA).

MXDR

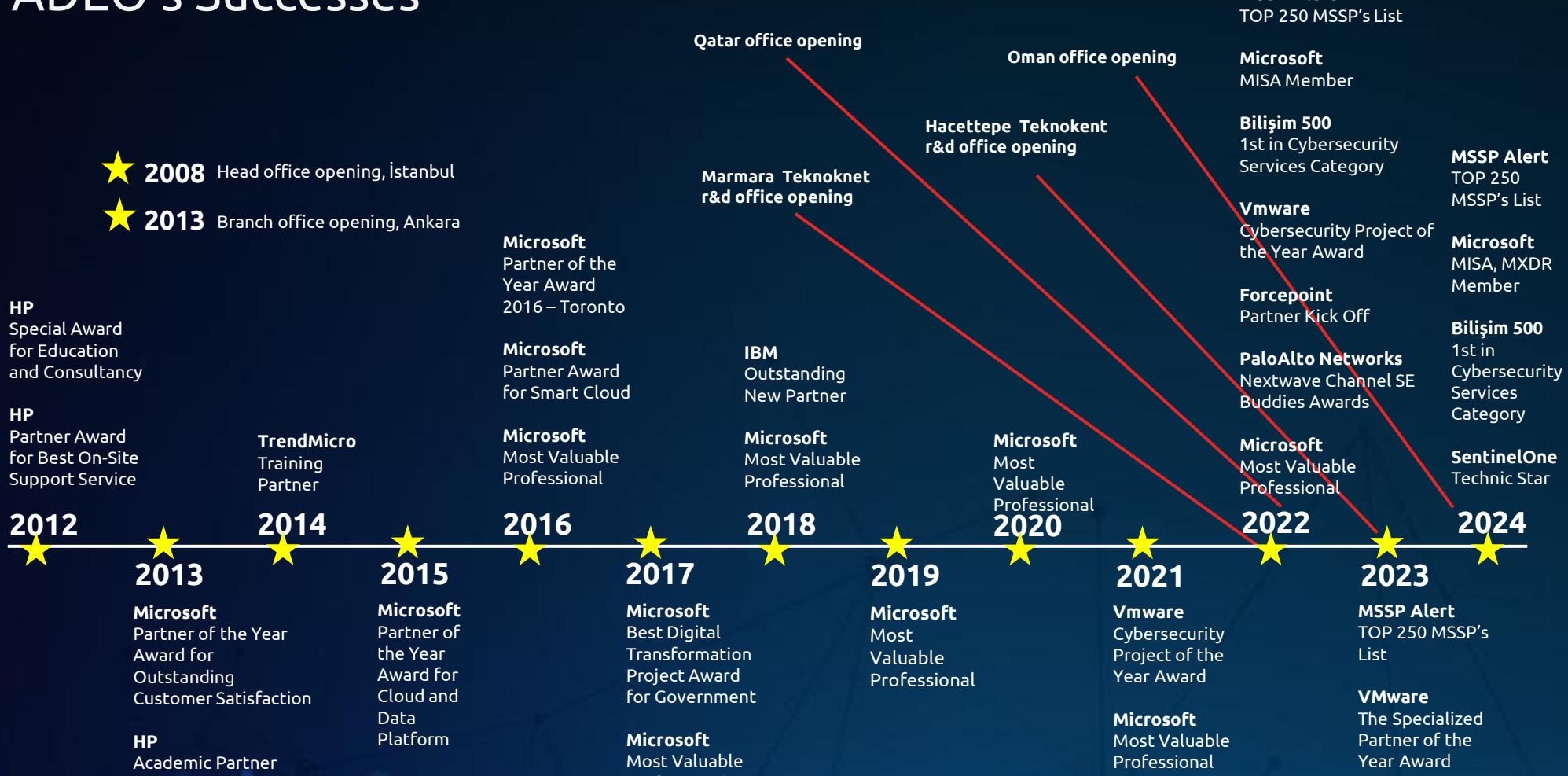
First Microsoft MISA, MXDR Partner, (2024)
(In the CEMA region, among 109 firms with this expertise, it holds the 1st position.

The Managed Extended Detection and Response (MXDR) service, approved by Microsoft, is a comprehensive security service that works as an extension of your team, allowing you to access expert resources around the clock. Monitoring your environment and prioritizing incidents requiring urgent intervention in a timely manner are critical for maintaining a robust security posture. Unlike traditional security models, MXDR combines data collection, correlation, continuous threat hunting, and incident response into a single managed service. Essentially, it is a holistic security solution that combines technology and human expertise to protect organizations against cyber threats.

Firsts in ADEO and in Turkey

- The First Digital Forensics Lab in Turkey, 2015
- Member of Turkey Cyber Security Cluster, 2018
- The First Carbon Black MSSP Partner in Turkey, 2019
- The First MDR Service Provider in Turkey, 2020
- The First Palo Alto Networks, MSSP Partner in Turkey, 2020
- (is also one of the 11 companies in the world with this competence.)
- The First Microsoft MSSP Partner in Turkey, 2021
- (ranks 2nd in the region, and 8th in the world.)
- The First Microsoft, MISA Member in Turkey, 2022
- MSSP Alert, TOP 250 MSSP's List, 2022 & 2023 & 2024
- 2022 - ADEO Cyber Security has achieved significant success by being recognized and listed among the top 250 Managed Security Services Providers (#MSSPs) globally, as compiled by MSSP Alert.
- 2023 - Adeo Cyber Security, a powerhouse in managed security services, just soared 47 spots in this year's Top 250 MSSP rankings.
- 2024 - Adeo Cyber Security, a powerhouse in managed security services, just soared 24 spots in this year's Top 250 MSSP rankings
- The First ADTR Service Provider in Turkey, 2023
- The First APTR Service Provider in Turkey, 2023
- The First Microsoft MISA, MXDR Member in Turkey, 2024
- (is also 1st of the 109 companies in the CEMA region with this competence.)
- Bilişim 500 1st in Cybersecurity Services Category 2023 & 2024
- SentinelOne Technic Star 2024

ADEO's Successes



ADEO CYBER SECURITY

www.adeosecurity.com

 ADEO Cyber Security Services

 @adeocomtr

 ADEOcomtr

 @adeocomtr

 @adeocomtr