ADEO
CYBER SECURITY

2023 Threat Report

TABLE OF CONTENTS

About 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.

About ADEO

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.

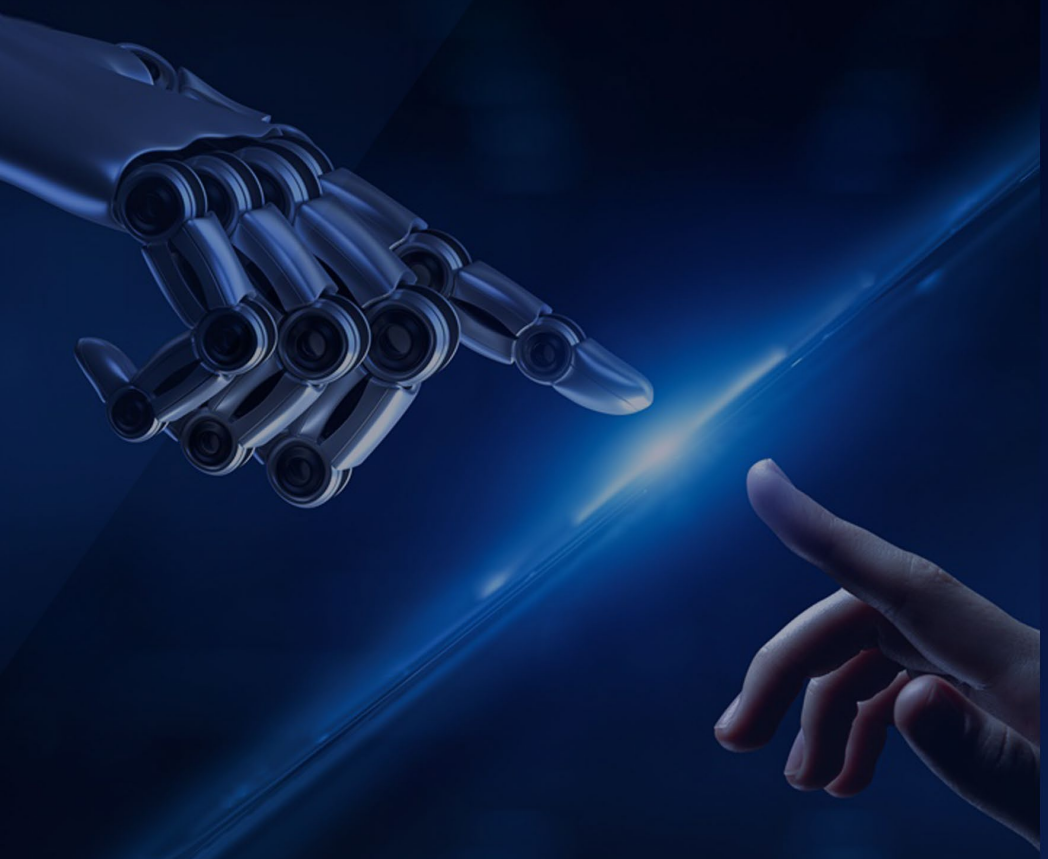
Dynamic Not Static

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

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.

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 2023 Threat Report: Cyber Security Analysis of 2023

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 2023. 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 2023 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.

ADEO
CYBER SECURITY

What Did We Do in 2023?

2023 Year Statistics

Most Targeted Sectors and Their total Number of Incident:

Retail:
10
Aviation:
5

Busiest Day:

13 June
Number of Alarms Reviewed This day:
3886

INCIDENT:
Attacker activities that require in-depth analysis and incident response processes as a result of analyzing a true detected alarm. They are mostly activities that spread and persist in more than one machine in a short time.

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

Total Number of Rules Developed 5000+

The number of **IOCs**, which was **51,000** in January 2023, was increased to **120,000** by the end of the year.

The number of detection rules, which was **4,000** in January 2023, was increased to **5,000** by the end of the year.

The number of **IOCs** scanned with threat intelligence from internal and external sources: **120,000**

Most Used Initial Access Technique

Exploit Public-Facing Application

%39,28

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.

Daily Routine of MDR Team

98% of inspected alarms are analyzed by **ADEO MDR** teams without notifying customers. **Necessary procedures** are applied according to the maturity of the product used. In this way, our customers can safely focus on their daily workflows. The analyzes made and the actions taken are reported and communicated to the customers at certain periods.

An average of **10 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

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.

2% of alarms are confirmed and necessary actions are taken after confirmation.

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.

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.

The distribution of initial access techniques requiring incident response in 2023 is indicated on **page 36**.

Number of Incident Response
28

INCIDENT MANAGEMENT STAGES

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 **11 minutes 19 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 **2023**, the mean **response time** of **ADEO MDR** team to **high severity** and **critical** incidents was **27 minutes 31 seconds**.

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

SECURITY BREACH
↓
DETECTION
↓
ANALYSIS
↓
RESPONSE
↓
REMEDIATION

Annual Alarm Numbers and Levels

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

Within the scope of these works, **the target for 2024** is:

- To reduce the number of critical and high-level alarms and,
- To increase the number of true positive alarms.

Detection and Response Time

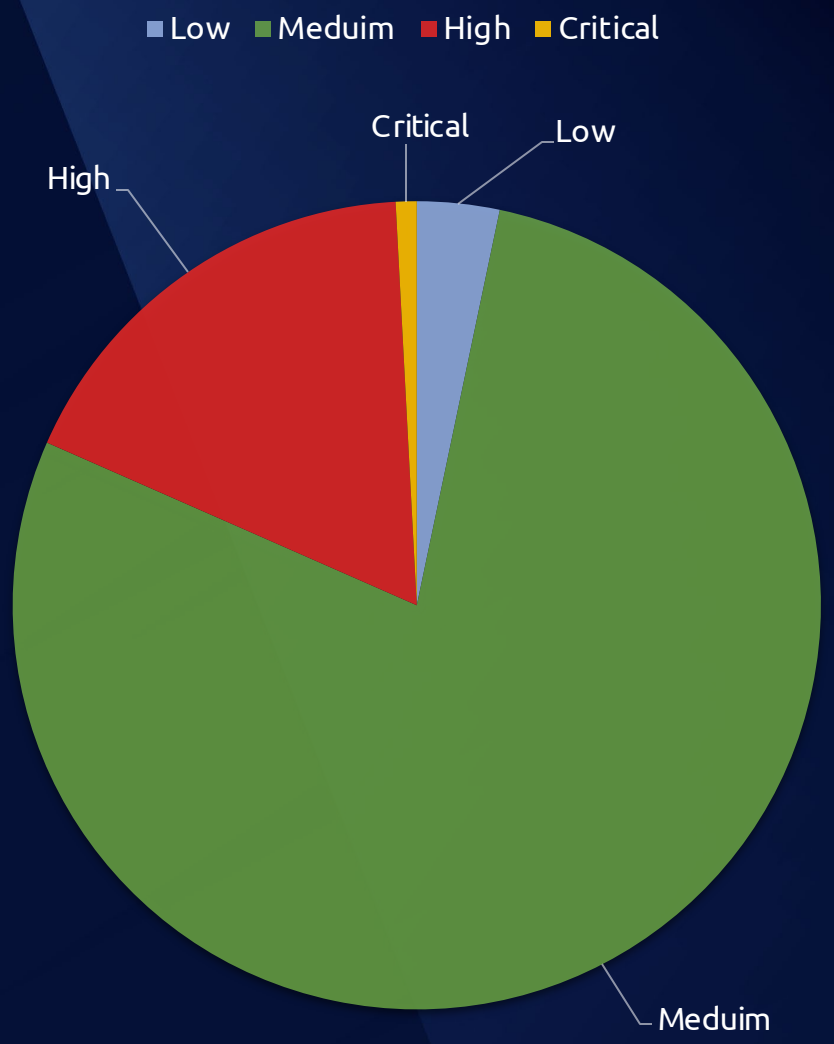
11m 19s
Mean Time to Detection

27m 31s
Mean Time to Response

In 2022, the highest number of alarms received on a single day was **652**, while this number was reported as **3886** on the busiest day of **2023**.

Annual Alarm Numbers and Levels

The mean detection time of only high severity and critical alarms was **11 minutes 19 seconds**, and the mean response time was **27 minutes and 31 seconds**.

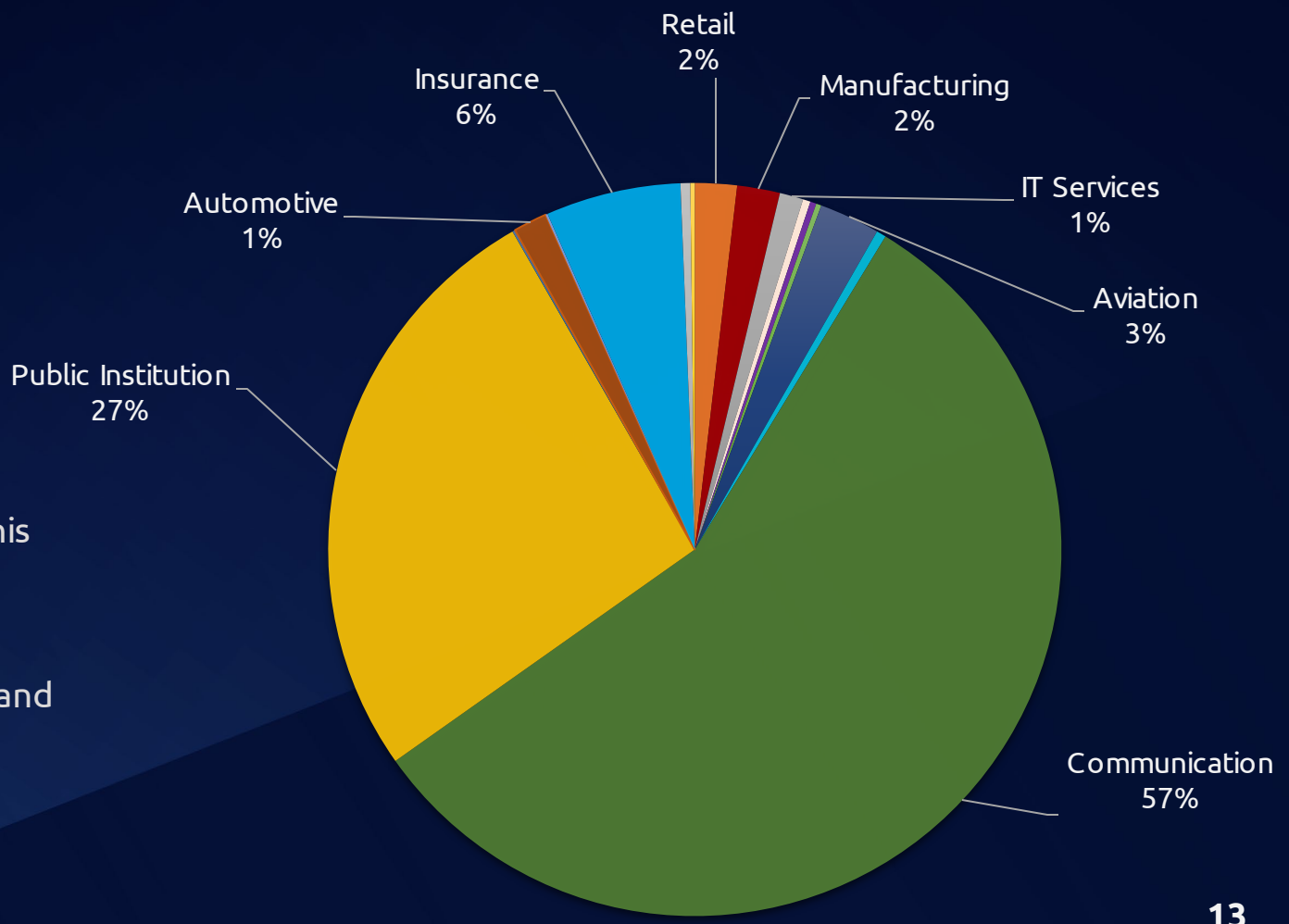


DETECTION TIME:
It is the time elapsed between the realization of the attack and the detection of the attack by the MDR team and defining it as an attack.

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:
It is a distributed sector in which employees are mostly in the field. The attacks were exposed due to this distributed structure.

PUBLIC INSTITUTION:
In 2023, due to geopolitical events and the election agenda, an increase in alarms has been observed in public institutions and organizations.

Sectors with the Highest Number of Incidents

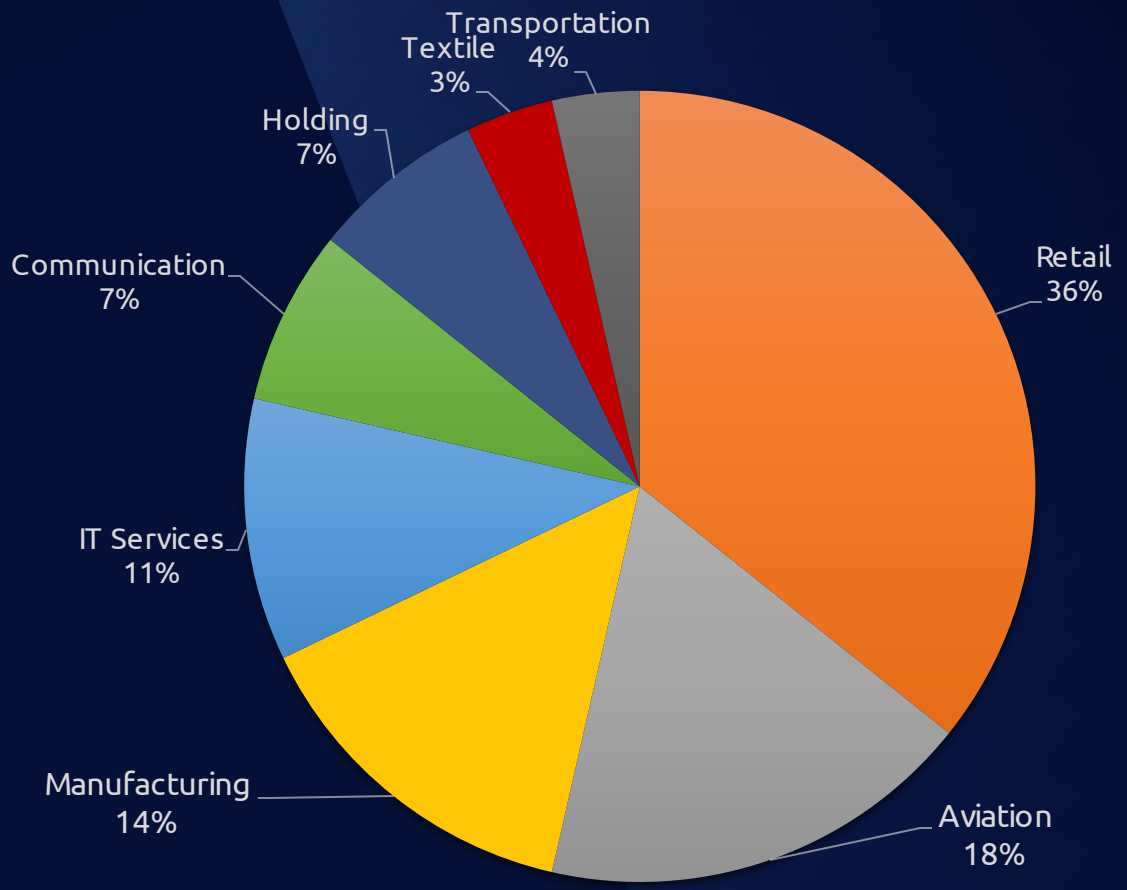
Due to the economic activity experienced in 2023, companies in the **retail** sector have become targets of various hacker groups. However, it has been observed that companies prioritize **red team** activities to test **their own internal dynamics**.

Retail activities in this sector are particularly important to pay attention to, both in terms of **business continuity and attack surface**.

Store systems are critical to a company's cybersecurity as they directly impact workflow and are vulnerable and often overlooked systems.

Therefore, companies in the retail sector should invest in **24/7 monitoring and incident response** to ensure the security of end-to-end systems.

Why the RETAIL sector?



Important Security Vulnerabilities Experienced in 2023 and ADEO MDR Service's Detection Rules

The rules we wrote as **ADEO MDR** about the important **Top 15+** vulnerabilities published in **2023** 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 2023 and ADEO MDR Service's Detection Rules

Security Vulnerability	Number of Rules Written	Number of IOCs Added
CVE-2023-22809 - Privilege Escalation Vulnerability	4	30
Possible KeePass [CVE-2023-24055] Exploitation Patterns (via powershell)	4	10
(CVE-2022-21894): Secure Boot Security Feature Bypass Vulnerability	8	50
Forta GoAnywhere Zero-Day	5	30
CVE-2023-23397 - Microsoft Outlook Privilege Escalation	15	20
3CXDesktopApp Supply Chain Attack	10	80
Rorschach - Ransomware via XDR Agent	3	4
CVE-2023-21554 - (QueueJumper) — Unauthorized Remote Code Execution	3	9
Novel Malware Persistence Within ESXi Hypervisors	8	31
MOVEit 0Day	10	70
Potential CVE-2023-36884 Exploitation Dropped File	3	13
Possible Outlook Reminder Persistence Attempt [CVE-2023-23397] (via powershell)	4	15
Credentials Harvest from Vulnerable CVE-2023-26258 Arcserve Unified Data Protection (UDP) [via register_event]	3	30
Exploiting Potential Barracuda ESG Zero-Day Vulnerability (CVE-2023-2868) Provides Persistence Through Scheduled Task (via file_event)	9	124
Possible PaperCut CVE-2023-27350 Exploitation Attempt (via cmdline)	4	17
Possible CVE-2023-21716 Microsoft Word Vulnerability Exploitation Patterns (via cmdline)	4	10
Amazon's AWS SSM agent can be used as post-exploitation RAT malware	8	10
New Collide+Power side-channel attack impacts almost all CPUs Vulnerabilities	8	5

Important Security Vulnerabilities Experienced in 2023 and ADEO MDR Service's Detection Rules

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.

Important Security Vulnerabilities Experienced in 2023 and ADEO MDR Service's Detection Rules by Numbers

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 **90 minutes.**

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

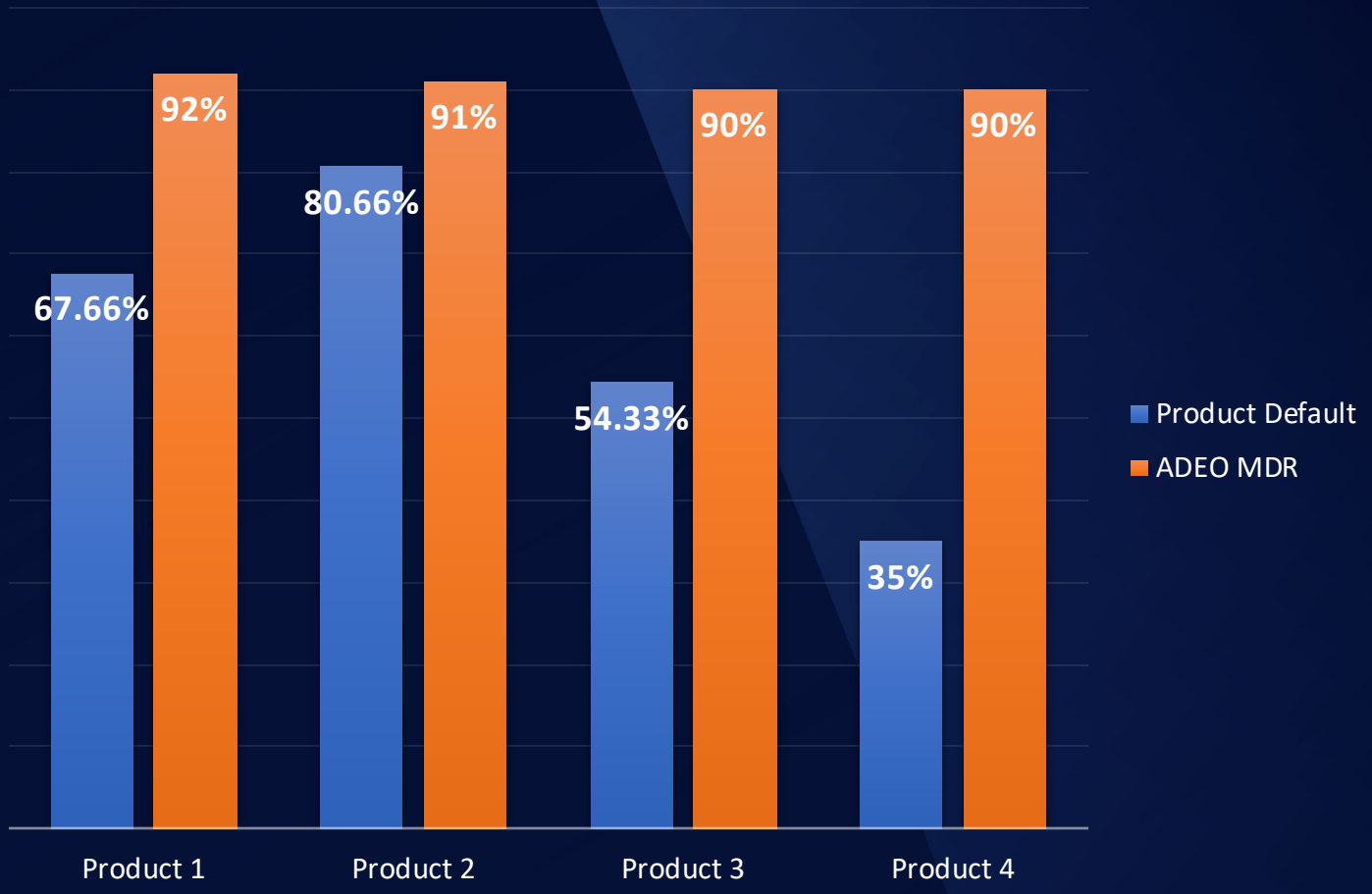
As a result of the work conducted by ADEO MDR team, it has been determined that the detection mechanisms of EDR/XDR need improvement. It is highly crucial to enhance and keep up-to-date EDR/XDR solutions according to the structure of the organization, potential threats, and attacks they may face, perform 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 5 minutes by utilizing accurate and precise information obtained directly from the field and through the creation of EDR/XDR rules.

Important Security Vulnerabilities Experienced in 2023 and ADEO MDR Service's Detection Rules by Numbers

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.



Important Security Vulnerabilities Experienced in 2023 and ADEO MDR Service's Detection Rules by Numbers

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.

Detection Rule Number Comparisons by Years

Number of Rules in 2021: increased from **600 to 2.000**

Number of Rules in 2022: increased from **2.000 to 4.000**

Number of Rules in 2023: increased from **4.000 to 5.000**

Major Steps in Cyber Security

The number of ADEO's detection rules is multiplying rapidly!

As ADEO, we continue to invest in cybersecurity and protect our customers against cyber attacks. In this context, we have achieved great success by **tripling the number of detection rules we have developed in the last two years**.

ADEO MDR Service Detection Rule Numbers and Increases

The developed Detection Rules cover and follow the MITRE ATT&CK framework, which is based on Tactics, Techniques, and Procedures (TTPs). This provides protection against the most current methods of cyber attacks.

This increase in detection rules ensures that our customers are more proactively and effectively protected against cyber attacks. It contributes to faster and more efficient detection and response processes for cyber attacks. It minimizes the risks such as data loss, financial loss, and reputation damage that cyber attacks can cause.

2021
600 rules

2022
2000 rules

2023
4000 rules

As of January 2024
5000 rules

Top 6 Agenda of 2023

Busiest Day
June 13

The Number of Alarms Reviewed on June 13th
3886

Rules targeting current vulnerabilities are quickly added by monitoring global trends and tracking threat intelligence.

Top 6 Agenda of 2023
#TOP 1| Fortra GoAnywhere Managed File Transfer (MFT)

What is Fortra GoAnywhere Managed File Transfer (MFT)?

Fortra GoAnywhere Managed File Transfer (MFT), enables organizations to securely, automatically, and traceably transfer their files and data. The platform offers security features such as encryption and authentication; it saves time and effort with functions like automatic file transfers and detailed logging. GoAnywhere MFT provides fast and reliable file transfer with its UDP-based solution and can be integrated with the cloud through the MFTaaS option.

What is CVE-2023-0669 – Fortra GoAnywhere Managed File Transfer (MFT) Remote Code Execution (RCE) Vulnerability?

This vulnerability has a CVSS score of 7.2 and a severity rating of "High". It was disclosed on February 6, 2023.

Between January 28, 2023, and January 30, 2023, it was discovered that an unauthorized party utilized a zero-day remote code execution (RCE) vulnerability to gain access to certain GoAnywhere customers' systems.

It was found that the unauthorized party used CVE-2023-0669 to create unauthorized user accounts in some MFTaaS customer environments.

In Fortra (formerly HelpSystems) GoAnywhere MFT, there is a pre-authentication command injection vulnerability in the License Response Servlet due to the serialization of an arbitrary object controlled by the attacker.

What are the activities of the CVE-2023-0669 – Fortra GoAnywhere Managed File Transfer (MFT) Remote Code Execution (RCE) Vulnerability Attack?

It was found that the unauthorized party utilized CVE-2023-0669 to install up to two additional tools, namely "Netcat" and "Errors.jsp", in some MFTaaS customer environments between January 28, 2023, and January 31, 2023.
The Cl0p ransomware group exploited this vulnerability in their activities in 2023.

For how long did we update the custom detection rules we created?

As ADEO MDR Service, we recreated the behaviors regarding the CVE-2023-0669 – Fortra GoAnywhere Managed File Transfer (MFT) Remote Code Execution (RCE) vulnerability in our own laboratory environments and used different patterns to detect relevant behaviors. **A total of 5 detection rules and 30 IOCs** were transferred to all our customers **within 2 hours.**

Top 6 Agenda of 2023
#TOP 2| PaperCut NG/MF

What is PaperCut NG/MF?

PaperCut NG/MF enables organizations manage and optimize their printing tasks.

What is CVE-2023-27350– PaperCut NG/MF Security Vulnerability?

On March 20, 2023, a critical security vulnerability named CVE-2023-27350 was discovered. This vulnerability has a CVSS score of 9.8 and is rated as "Critical". This indicates that the vulnerability is extremely dangerous and needs to be addressed urgently.

The vulnerability allows attackers to bypass authentication in PaperCut MF/NG software and execute code with SYSTEM privileges. This enables attackers to gain full control over affected systems, conduct data theft or ransomware attacks, and cause system compromise. It is known that the Cl0p Ransomware group actively exploits this vulnerability.

What are the effects of CVE-2023-27350 vulnerability?

It has been utilized by the Cl0p Ransomware group. Since code will be executed with SYSTEM privileges, the impact of the vulnerability is escalated to a larger scale.

For how long did we update the custom detection rules we created?

As ADEO MDR Service, we recreated the behaviors of CVE-2023-27350 - PaperCut NG/MF vulnerability in our own laboratory environments and used different patterns to detect relevant behaviors. **A total of 4 detection rules and 17 IOCs** were transferred to all our customers within **1.5 hours.**

Top 6 Agenda of 2023
#TOP 3| Dark Power Ransomware

Dark Power Ransomware Group is a new ransomware group that emerged in February 2023. It quickly gained attention by targeting Turkey and using ransomware written by NIM.

Most Affected Countries and Sectors?

It has been determined that the Dark Power Ransomware group operates in many areas. Some of the sectors it targets include education, healthcare, and manufacturing. Attacks by Dark Power have been detected in countries such as the United States, Peru, Turkey, France, Israel, Egypt, and Algeria.

What are Dark Power's 2023 activities?

It has been determined that Dark Power attacked 10 different organizations in February alone. We can say that it poses a global threat due to the diversity of the countries it targets.
They have written their malware with Nim, which is a relatively new and increasingly popular multi-platform language among ransomware groups. They use the Nimcrypto library to encrypt files. They save encrypted files with the extension "dark_power".

Dark Power has set the ransom amount to be paid by hacked institutions as 10,000$ worth of XMR (Monero). They state that if the ransom amount is not paid, they will publicly release the seized data within 72 hours. Dark Power generally uses the phishing attack technique when targeting users.

For how long did we update the custom detection rules we created?

As ADEO MDR Service, we recreated the behaviors of the Dark Power ransomware group in our own laboratory environments and used different patterns to detect relevant behaviors. **A total of 2 detection rules and 27 IOCs** were transferred to all our customers **within 2.5 hours.**

Top 6 Agenda of 2023
#TOP 4| CVE-2023-23397 - Outlook Vulnerability

What is CVE-2023-23397 - Outlook Vulnerability?

The vulnerability has a CVSS score of 9.8 and a severity rating of "Critical". It was disclosed on March 14, 2023.

It is a security vulnerability that allows a threat actor to create a message (.msg) file with a custom PidLidReminderFileParameter property containing a Universal Naming Convention (UNC) path to a Server Message Block (SMB) server controlled by the attacker in Microsoft Outlook. The PidLidReminderFileParameter allows the sender to set a custom notification sound for items such as meeting reminders.

Connections to the SMB server controlled by the threat actor will result in the theft of the targeted user's Net-NTLMv2 hashes. The threat actor can then use these hashes to authenticate on other servers supporting NTLMv2 authentication or attempt to crack the hashes offline to obtain clear-text credentials. If attackers cannot access the NTLMv2 hash value via SMB, they also provide a connection via WebDAV.

The attack only requires the targeted user to receive an email. No user interaction is required for the exploitation (zero-click).

What are the effects of CVE-2023-23397 vulnerability?

This security vulnerability has been exploited by APT28 to target European organizations in the government, energy, and transportation sectors. The APT28 group, targeting Microsoft, is associated with Russia.

As a result, NTLMv2 hash information in clients using Microsoft Outlook (excluding web Outlook) may have been triggered and extracted through this vulnerability. This has had a significant impact worldwide and has been utilized in various government and state institutions, primarily in Poland. It can be assumed that this vulnerability will be used as a leverage in intergovernmental cyber warfare.

For how long did we update the custom detection rules we created?

As ADEO MDR Service, we recreated the behaviors of the CVE-2023-23397 - Outlook Security Vulnerability in our own laboratory environments and used different patterns to detect relevant behaviors. **A total of 10 detection rules and 22 IOCs** were transferred to all our customers **within 3 hours**.

Top 6 Agenda of 2023
#TOP 5| MOVEit SQL Vulnerability

What is the MOVEit application?

MOVEit Transfer (formerly known as MOVEit DMZ or MOVEit File Transfer) supports file and data exchange within and between organizations using a common shared folder with simple browser access for users; between servers, systems, and applications; and also, among groups and individuals.

What is CVE-2023-34362 - MOVEit SQL Vulnerability?

The vulnerability has a CVSS score of 9.8 and a severity rating of "Critical".

It is a SQL injection vulnerability in Progress Software's MOVEit Transfer web application that could allow an unauthenticated attacker to access the MOVEit Transfer database. Depending on the database engine used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker could extract information about the structure and content of the database and execute SQL queries that modify or delete database elements.

What are the effects of CVE-2023-34362 - MOVEit SQL Vulnerability?

It has been utilized by the Cl0p Ransomware group. Cl0p is a Russia-linked ransomware gang. The SQL injection vulnerability has resulted in ransomware attacks on numerous organizations.

Who were targeted in MOVEit attacks?

Clop is a ransomware gang linked to Russia. While it's not clear who infiltrated federal agencies in the U.S., it was revealed that the ransomware gang known as Clop has been exploiting vulnerabilities in MOVEit software to attack hundreds of organizations in recent weeks, including universities, banks, and large multinational companies. The UK's communications regulator Ofcom also stated that some confidential information had been compromised in MOVEit cyberattacks. The agency confirmed in a statement that certain data related to companies and personal information of 412 Ofcom employees were breached as a result of the attacks orchestrated by hackers.

When listing the countries where the MOVEit security vulnerability was exploited, it was found that 72.2% of the known compromised entities were in the United States, 6.6% in Germany, and 3.9% in the United Kingdom and Canada combined.

For how long did we update the custom detection rules we created?

As ADEO MDR Service, we simulated the behaviors of CVE-2023-34362 - MOVEit SQL Vulnerability in our own laboratory environments and used different patterns to detect relevant behaviors. **A total of 10 detection rules and 70 IOCs** were transferred to all our customers **within 3 hours.**

Top 6 Agenda of 2023
#TOP 6| Barracuda Email Security Gateway

What is Barracuda Email Security Gateway?

Barracuda ESG (E-mail Security Gateway), Barracuda Email Security Gateway, manages and filters all incoming and outgoing email traffic, protecting organizations from email-based threats and data leaks. This service is known to be used by many organizations.

CVE-2023-2868- Barracuda Email Security Gateway Vulnerability

The vulnerability has a CVSS score of 9.8 and the severity value is determined as "Critical".

It is a remote code execution (RCE) vulnerability found in the Barracuda Email Security Gateway (ESG) product. The Barracuda zero-day security flaw, identified as CVE-2023-2868, was officially disclosed on May 19, 2023, with a critical CVSS score of 9.8.

This vulnerability arises due to inadequate sanitization of the process used in handling ".tar" files. It stems from incomplete validation of the file names within the content of the ".tar" file provided by the user. An attacker can manipulate these file names in a specific format to successfully execute a remote system command via the Perl "qx" operator with the privileges of the Email Security Gateway product.

This means effectively unsanitized and unfiltered user-controlled input via a variable executed as a system command through Perl's qx{} routine.

What Are the Activities of the Barracuda ESG Zero-day Attack?

According to the analyses conducted, the initial exploitation date of this security vulnerability was determined to be October 10, 2022. This attack was carried out by the China-backed APT group UNC4841. It was reported that the Australian Capital Territory Government was affected by this attack. Additionally, according to Barracuda's statement, approximately 5% of devices worldwide were impacted.

For how long did we update the custom detection rules we created?

As ADEO MDR Service, we have recreated the behaviors of CVE-2023-2868 - Barracuda Email Security Gateway Vulnerability in our own laboratory environments and used different patterns to detect the relevant behaviors. **A total of 9 detection rules and 124 IOCs** have been communicated to all our customers **within 2.5 hours.**

ADEO
CYBER SECURITY

DFIR

ADEO DFIR 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

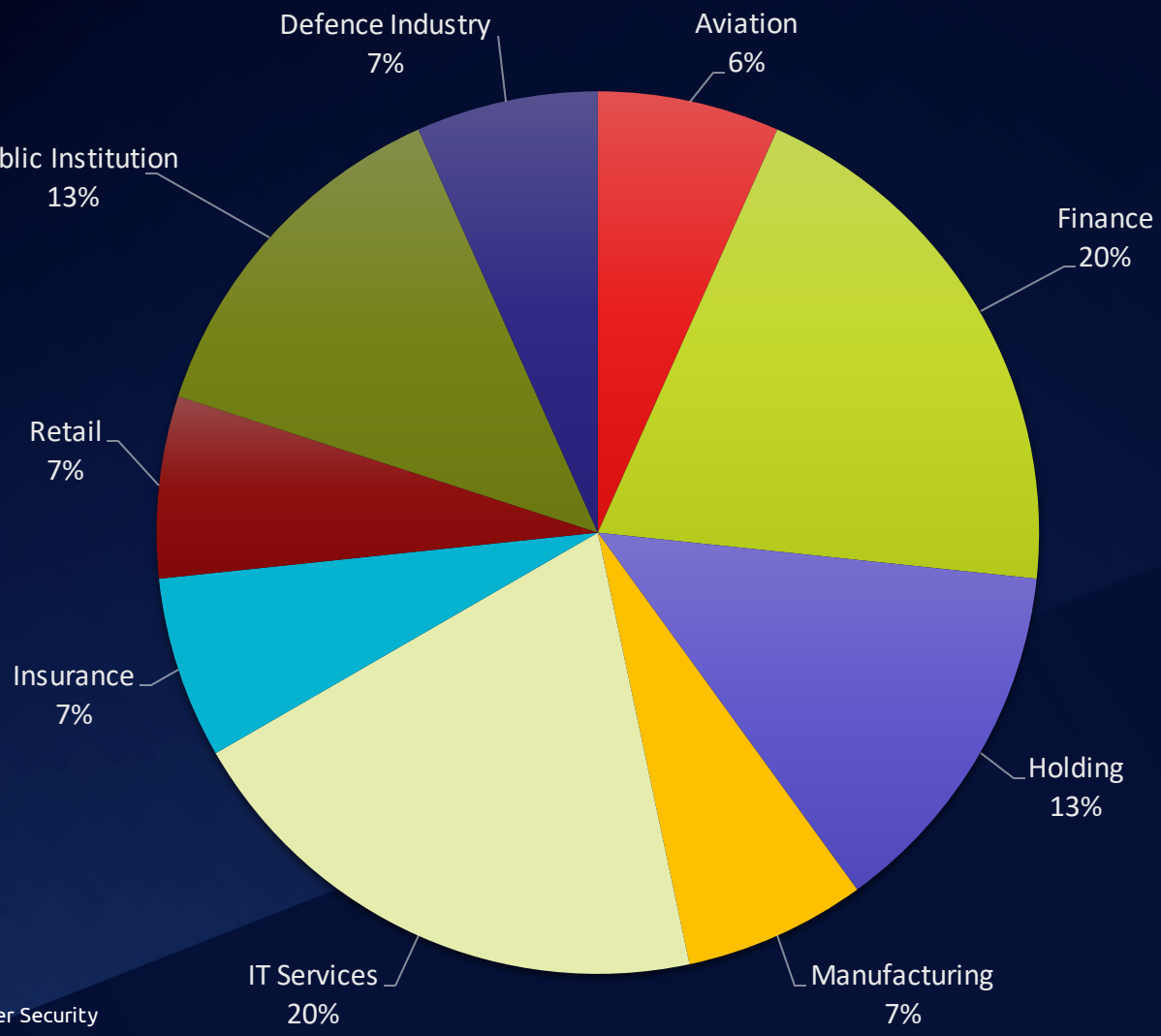
used by the attacking group are identified and thoroughly analyzed and reported.

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 DFIR Service

Distribution of Incidents by Sector in 2023:



Primary Cases Observed During Incidents:

Ransomware:

It has been observed that threat actors conduct encryption activities for the purpose of threat and extortion against current target individuals or institutions. After gaining initial access (Vulnerability Exploitation, Phishing, etc.), the attackers use reconnaissance tools (Nmap, theHarvester, etc.) to spread within the network (Credential Dumping-Mimikatz), carry out data exfiltration, and data encryption on as many devices as possible. They then communicate their demands to the organization via an email, requesting ransom.

- File and System Encryption
- Ransom Demands

Cyber Espionage:

Data exfiltration operations conducted by threat actors without any encryption activity or ransom demands have been encountered. Such activities, which are not directly converted into financial gains, can be categorized under "Cyber Espionage."

- Information Gathering
- Targeted Data Theft

E-mail Phishing:

It is a cyber attack technique particularly favored by cyber attackers for obtaining initial access and email tampering.

Subtitles:

- Data Encryption
- Data Exfiltration
- Data Corruption/Loss
- Crypto Miners
- Intrusion

Info Stealer Malware:

During the attacks, information theft activities targeting the victim were observed. The malicious software used during these activities can be categorized under the title of "Info Stealer Malware".

- Personal Identifiable Information (PII)
- Financial Information
- Credit Card Information etc.

Tactics and Techniques Used by Attackers in Observed Incidents:

Obfuscation:

Obfuscation, encountered frequently by attackers in the cases we've seen, is often preferred as an Anti-Forensics technique to evade detection tools and slow down the analysis process.

- Data Encoding/Encryption
- Adding Unnecessary Code

Spear Phishing:

It is a methodology applied in direct targeted attacks.

- Email-based
- Targeted Attacks

Vulnerability Exploitation:

It is the targeted exploitation of vulnerabilities found in systems and applications, especially those where recent patches have not been applied. Attackers also monitor some platforms where disclosed vulnerabilities are published (such as NVD, MITRE, etc.), and during attacks, they leverage information from these platforms to carry out malicious activities on unpatched/outdated target systems/applications.

Tactics and Techniques Used by Attackers in Observed Incidents:

Usually Remote Code Execution (RCE) Vulnerabilities

Spray&Pray:

- Within the scope of Vulnerability Exploitation
- Propagation and Evasion Approach

Lateral Movement:

- Identity Theft
- Inter-System Movement

Discovery:

- Network Scanning etc.
- Identification of Target Systems

Persistence:

- Backdoors
- Registry Changes
- Scheduled Tasks etc.

Methods of Earning Money for Attackers

- Ransomware
- Crypto Miners
- Data Theft and Sale
- Carding
- Blackmailing (DDOS Attack etc.)

Methods of Initial Access Observed

- External Remote Services/Exploit Public-Facing Application
- Phishing
- Malware
  - Reverse/Bind ShellCrypto Miners
  - Remote Control Tools (Ammyy Admin, Anydesk etc.)

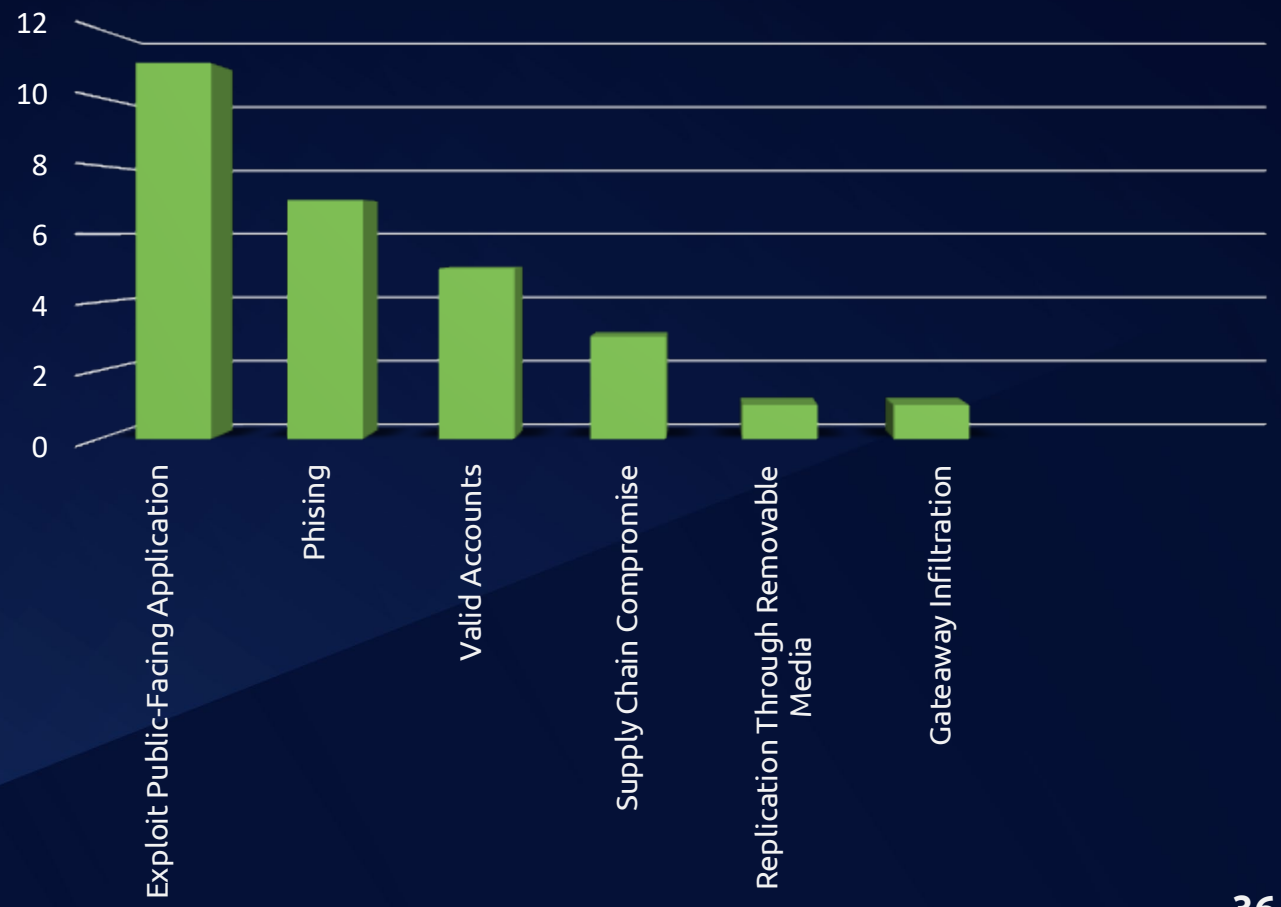
Most Used Initial Access Technique

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.

"Preventing the first access is important for the security of the system."



ADEO CYBER SECURITY

ADEO MDR Service

Tactics, Techniques and Detection Rules

Attack Detection Rules

Cyber Security Peak: ADEO's 94% 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.

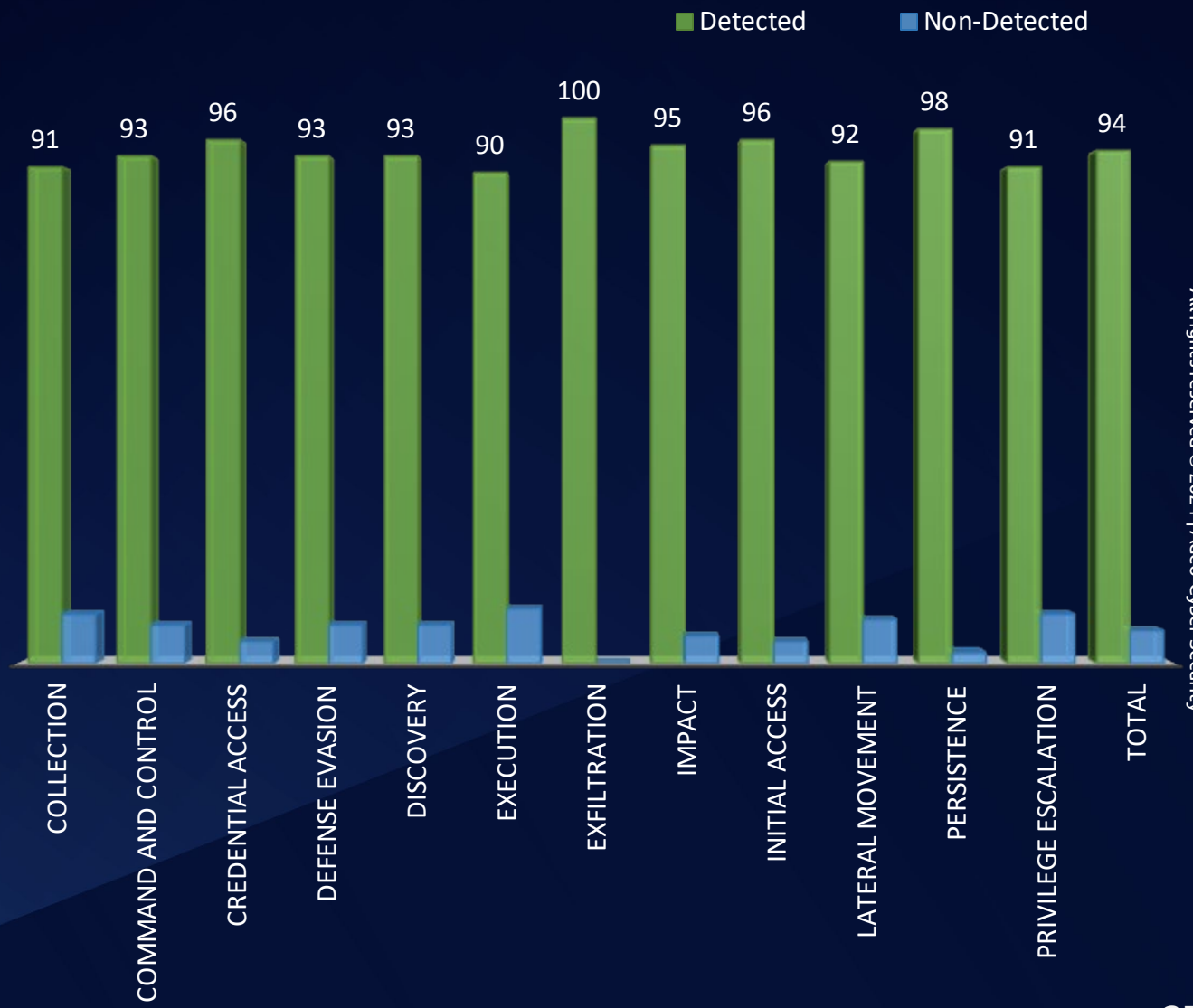
As ADEO, we use
- the latest technology and
- the expertise of the most competent analysts

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

Our service, **with a detection rate of 94%,** stands as a concrete demonstration of our expertise in the 2023 report.

After 11,507 instances of attack techniques in 2023, with reference to 12 MITRE ATT&CK TTP values, it is observed that **we have an average detection rate of 94%.**

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 94%.**



Tactics

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.

91% of the attacks made using the Collection tactic can be detected by our **ADEO MDR Service**.

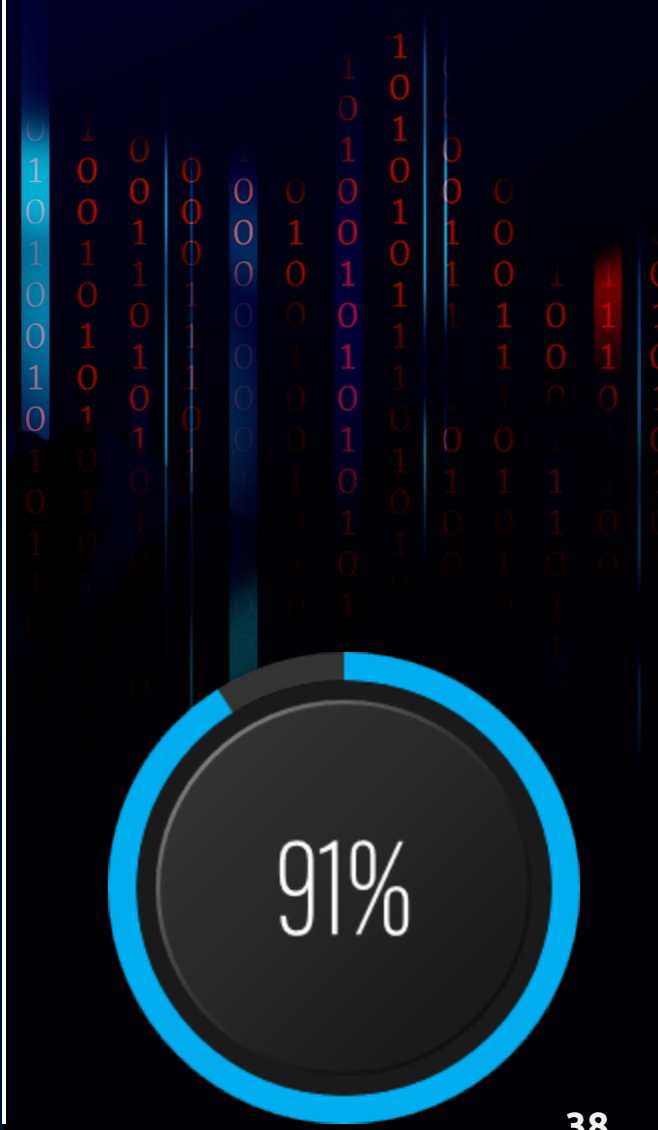
- **In addition to EDR technology**, it is recommended to implement data loss prevention systems for the detection of these and similar attacks. It is recommended to use **DLP technology**, which is an additional data leakage prevention system, for studies such as planning controls such as reducing the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



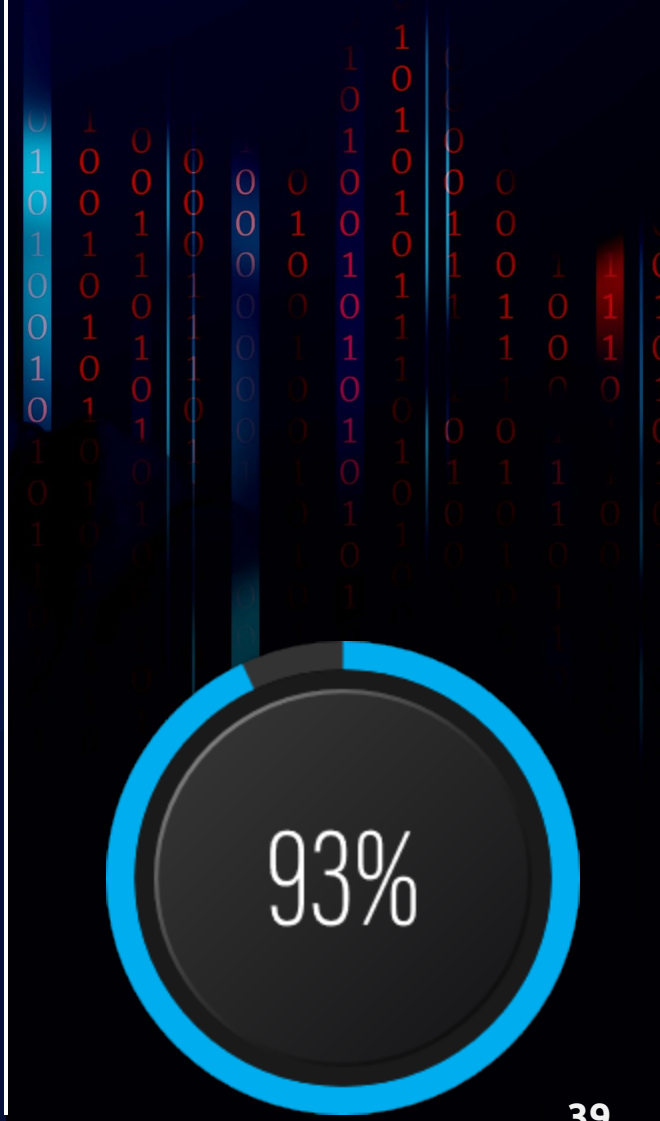
Tactics

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.

93% 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.



Tactics

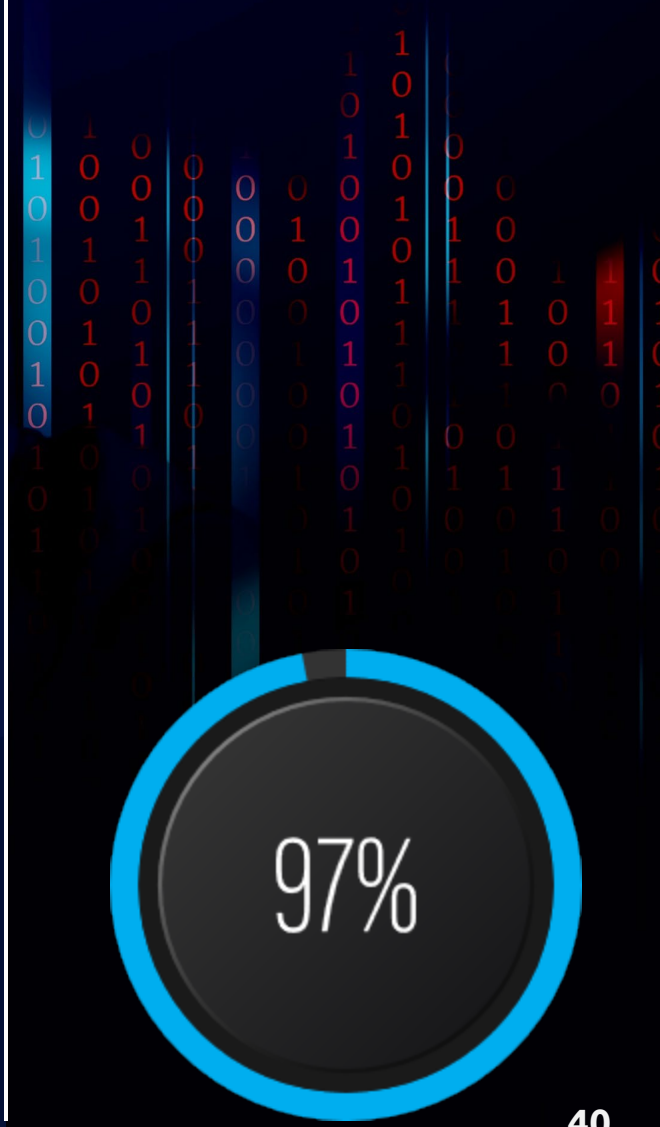
3.Credential Access

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.

97% 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.



Tactics

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.

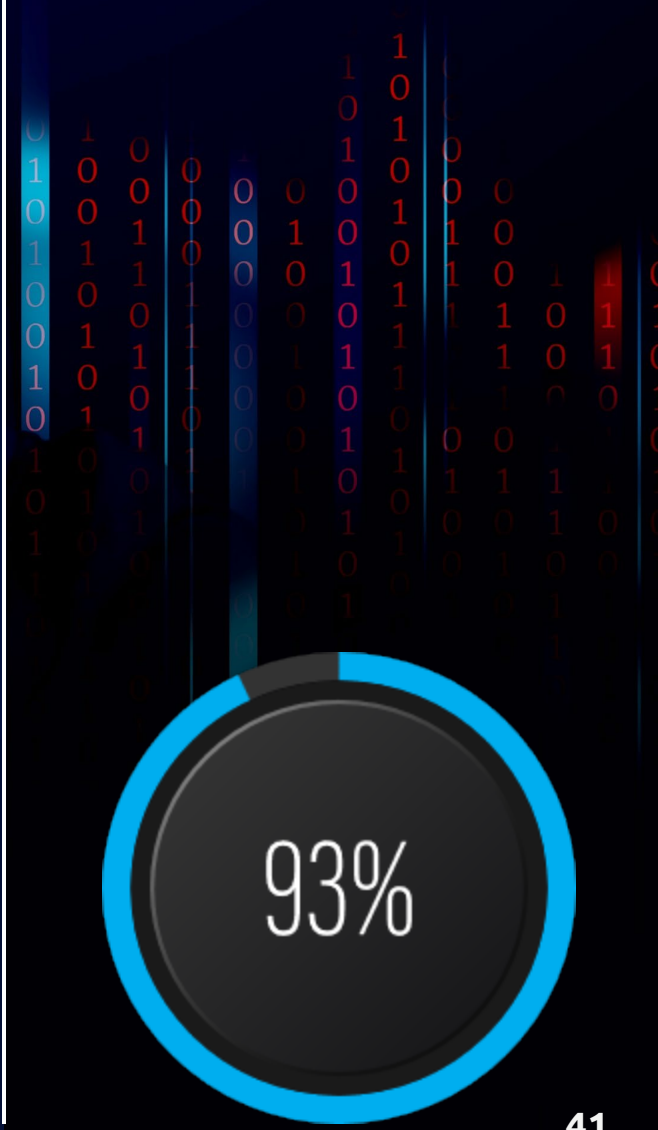
93% of the attacks made using the Defense Evasion tactic can be detected by our **ADEO MDR Service.**

- 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.



Tactics

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 howto 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.

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

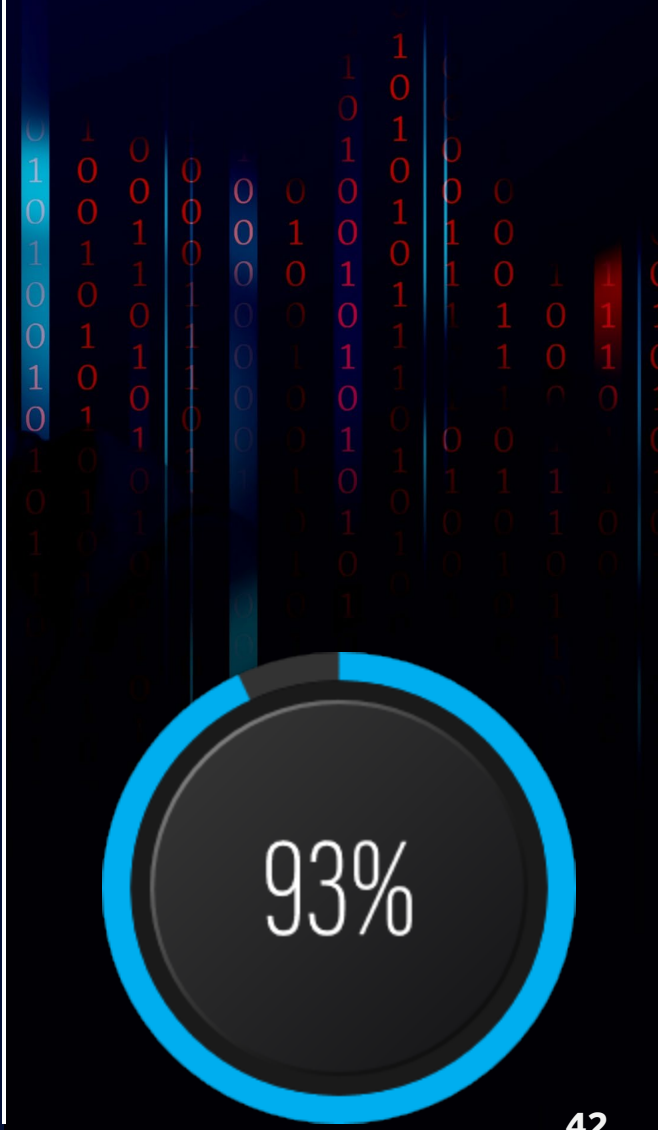
- The existing environment in the institutions (**with the help of Active Directory, Firewall, Network Segmentation** and other security devices, if any) should be tightened in accordance with the needs and **the attack surface should be narrowed.** It is recommended to tighten and mature the **Audit**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



Tactics

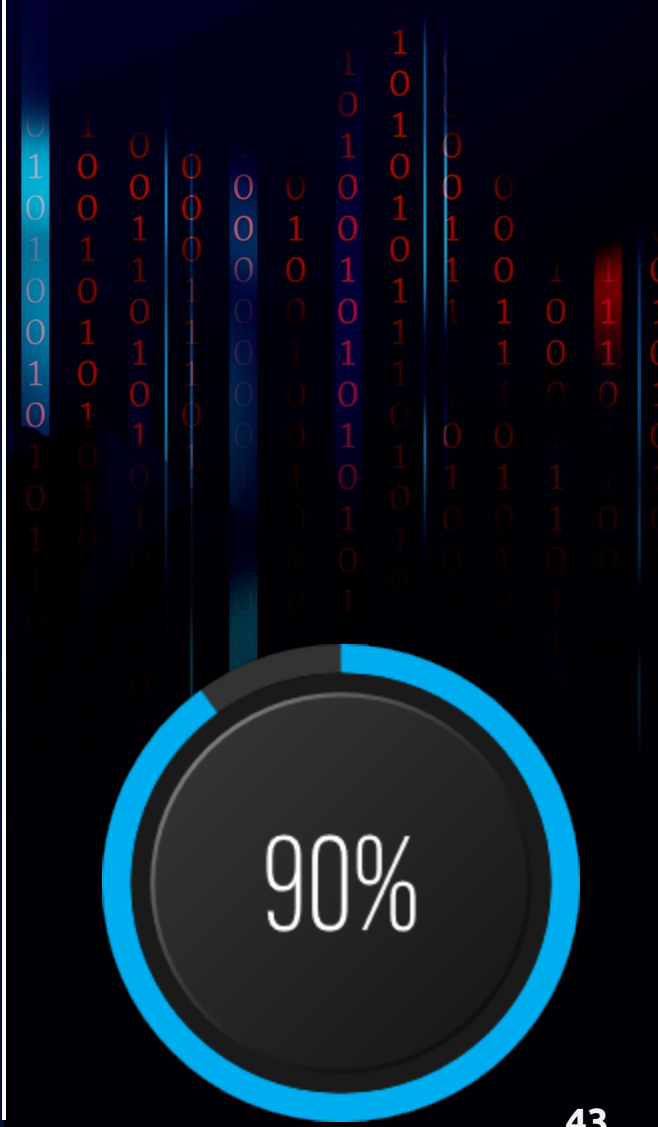
6.Execution

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.

90% 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.**



Tactics

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.

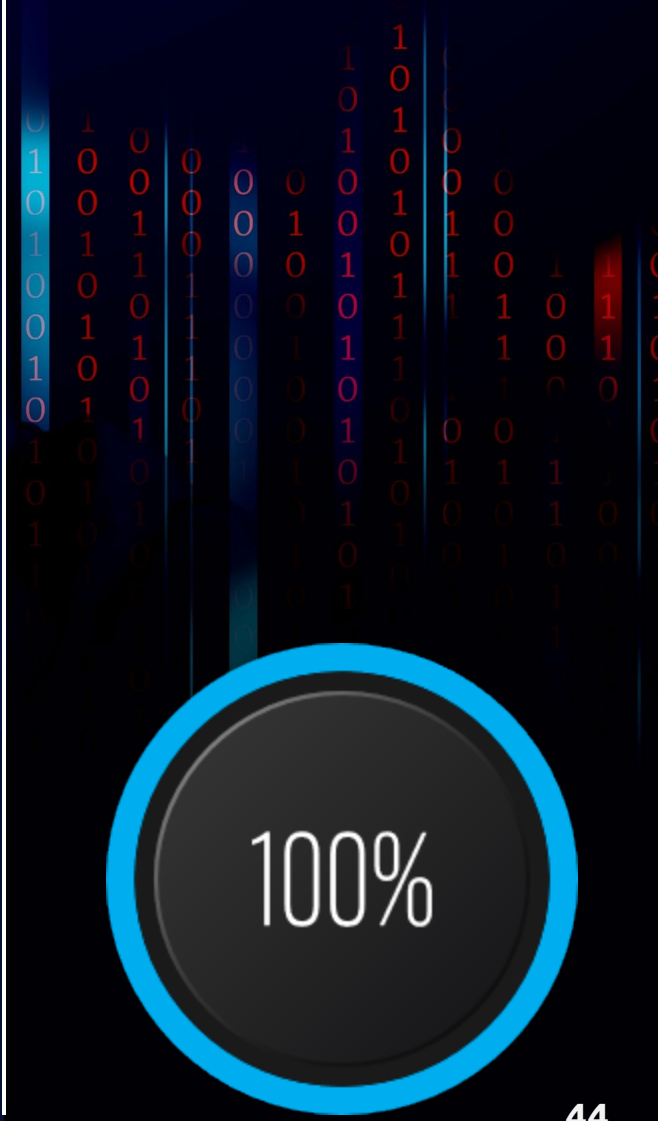
100% of the attacks made using the Exfiltration tactic can be detected by our **ADEO MDR Service.**

- 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.



Tactics

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.

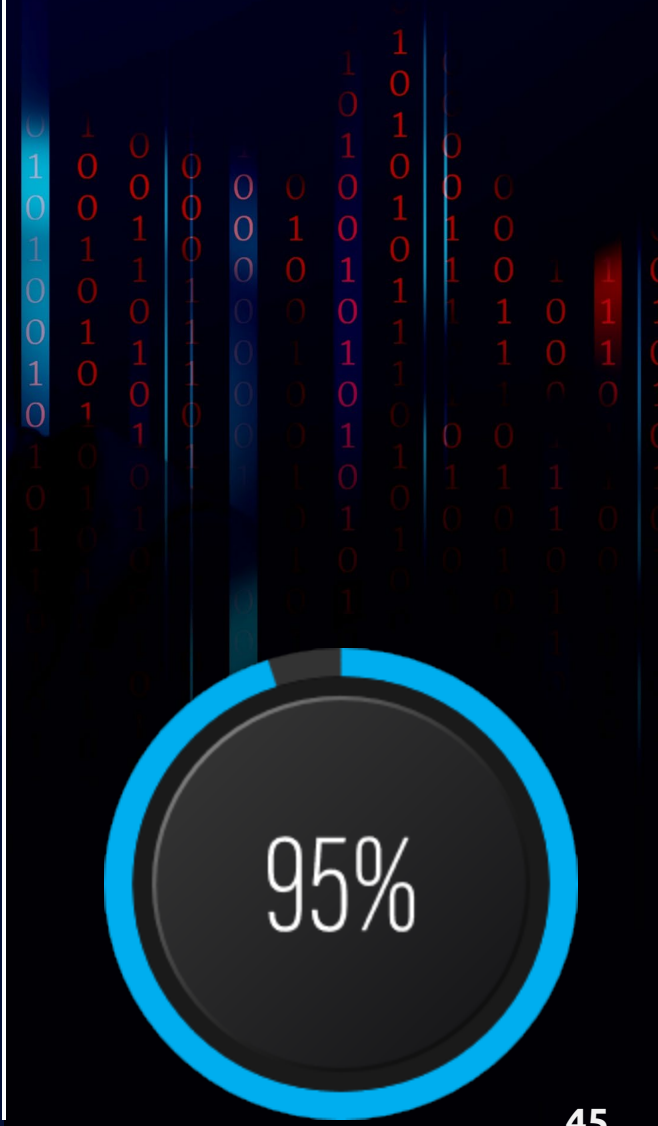
95% of the attacks made using Impact tactic can be detected by our **ADEO MDR Service.**

- **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.**



Tactics

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.

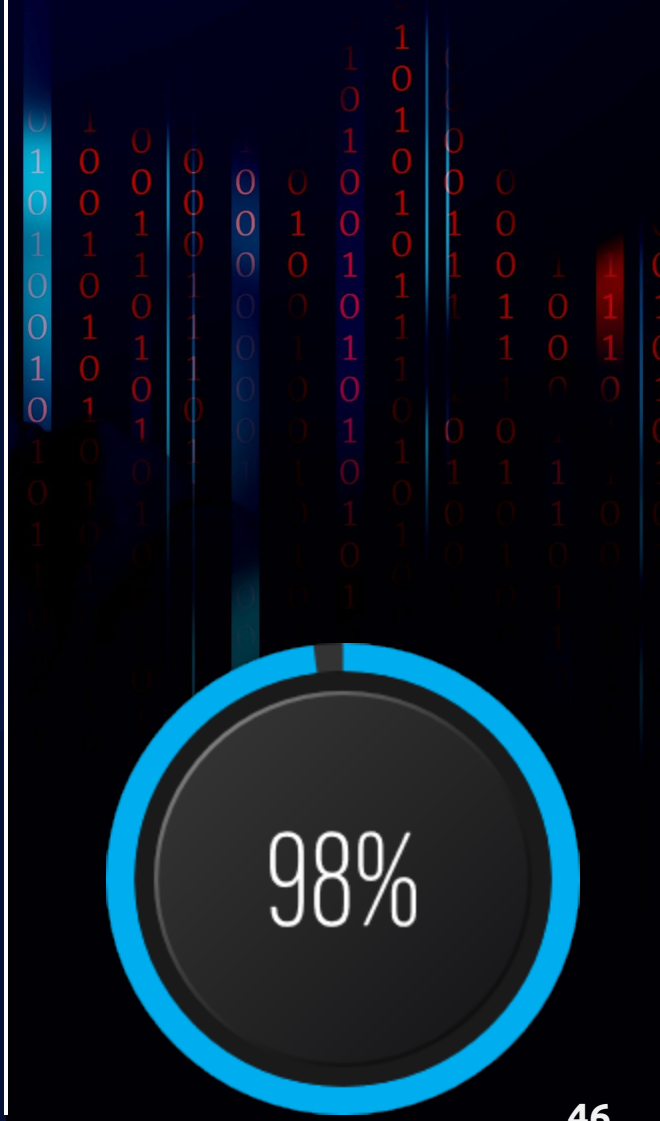
98% of the attacks made using the Persistence tactic can be detected by our **ADEO MDR Service.**

- **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.**



Tactics

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.

91% of the attacks made using the Privilege Escalation tactic can be detected by our **ADEO MDR Service.**

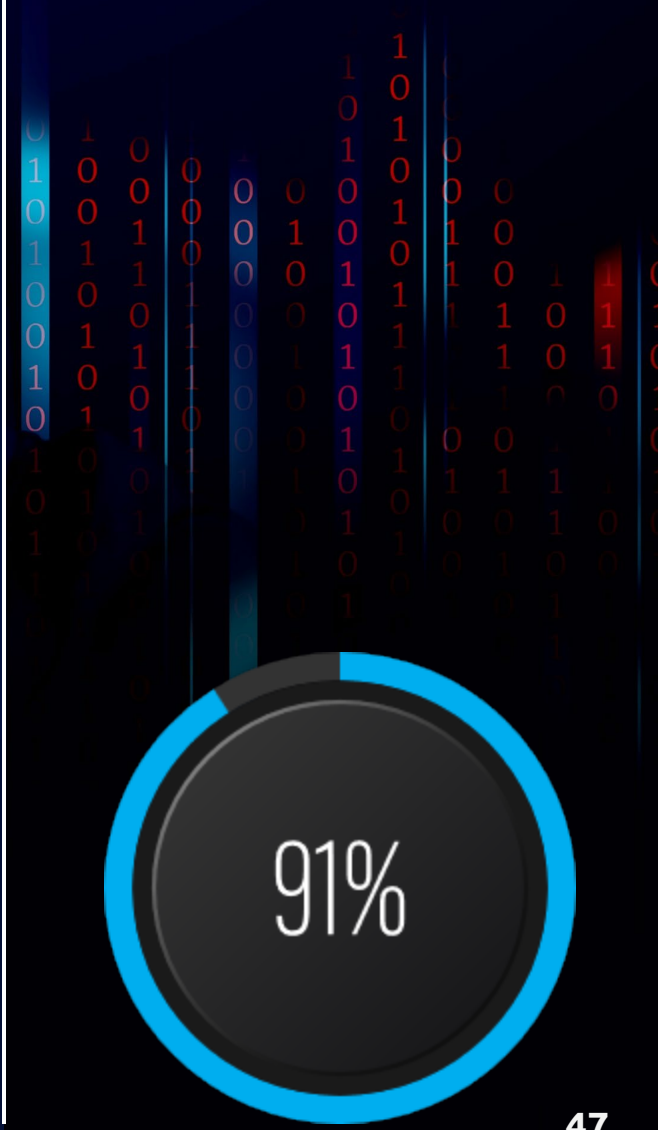
- Logs from directory servers such as **Active Directory (AD)** or **LDAP** need to be configured. User rights upgrade or new user creation events need to be followed. It is necessary to create a list of privileged user account names, authorizations. Privilege Escalation attacks or attacks against privileged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



Tactics

11.Initial Access

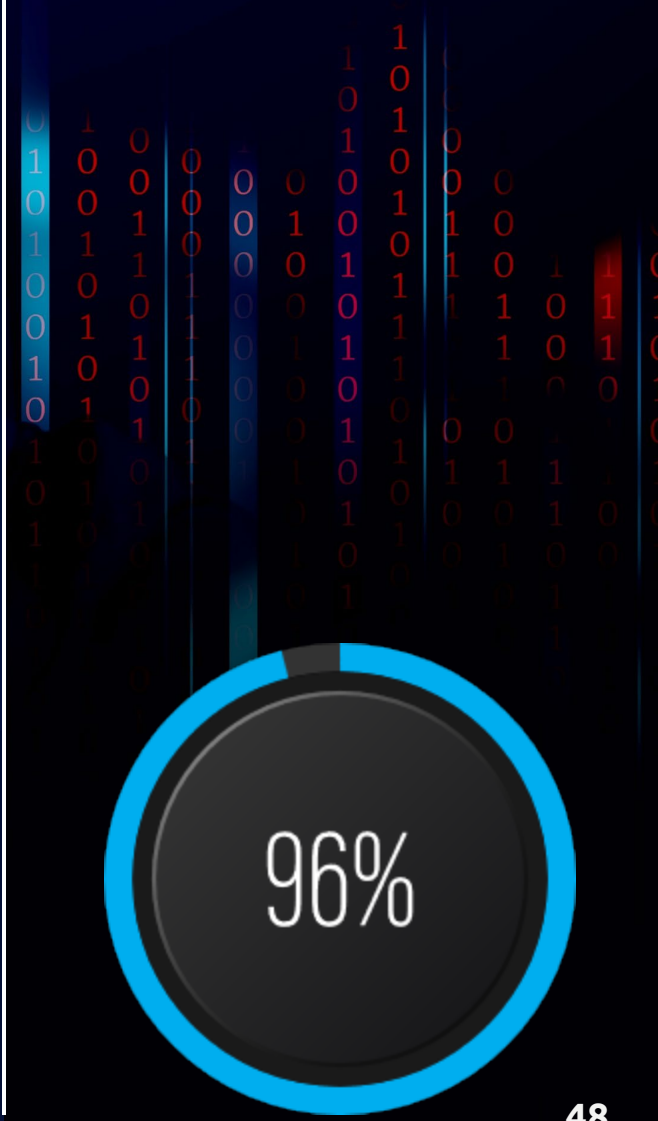
The adversary is trying to get into your network.

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.**



Tactics

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.

92% 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.

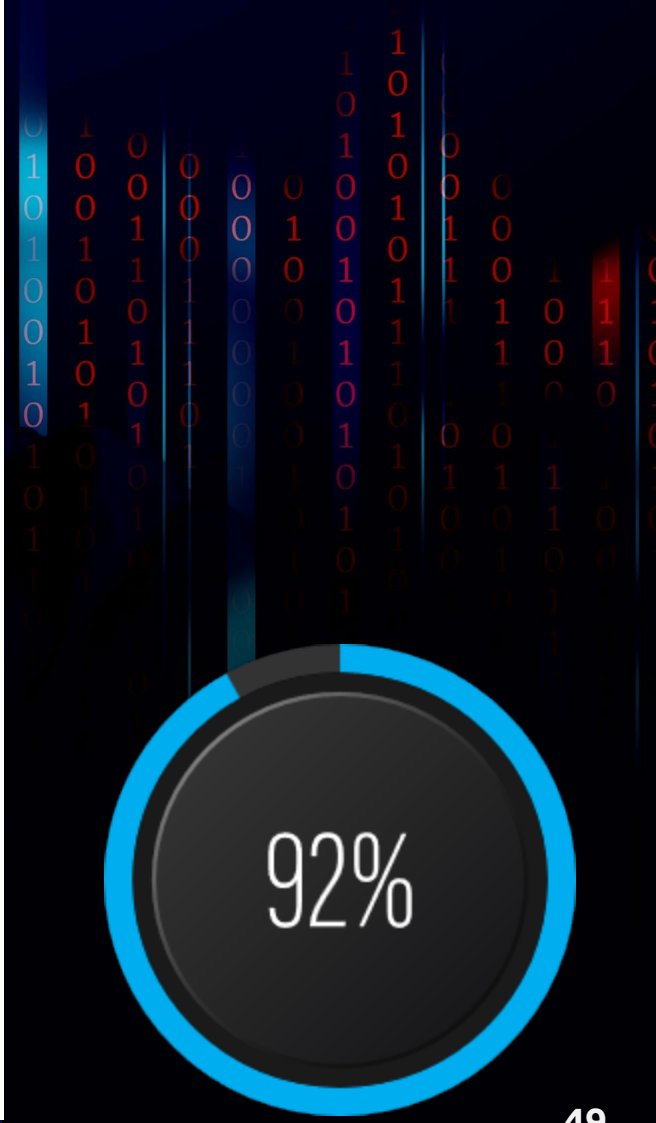
- **By isolating VLAN** networks from each other, it prevents the spread of attacks and data breaches.

- 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.



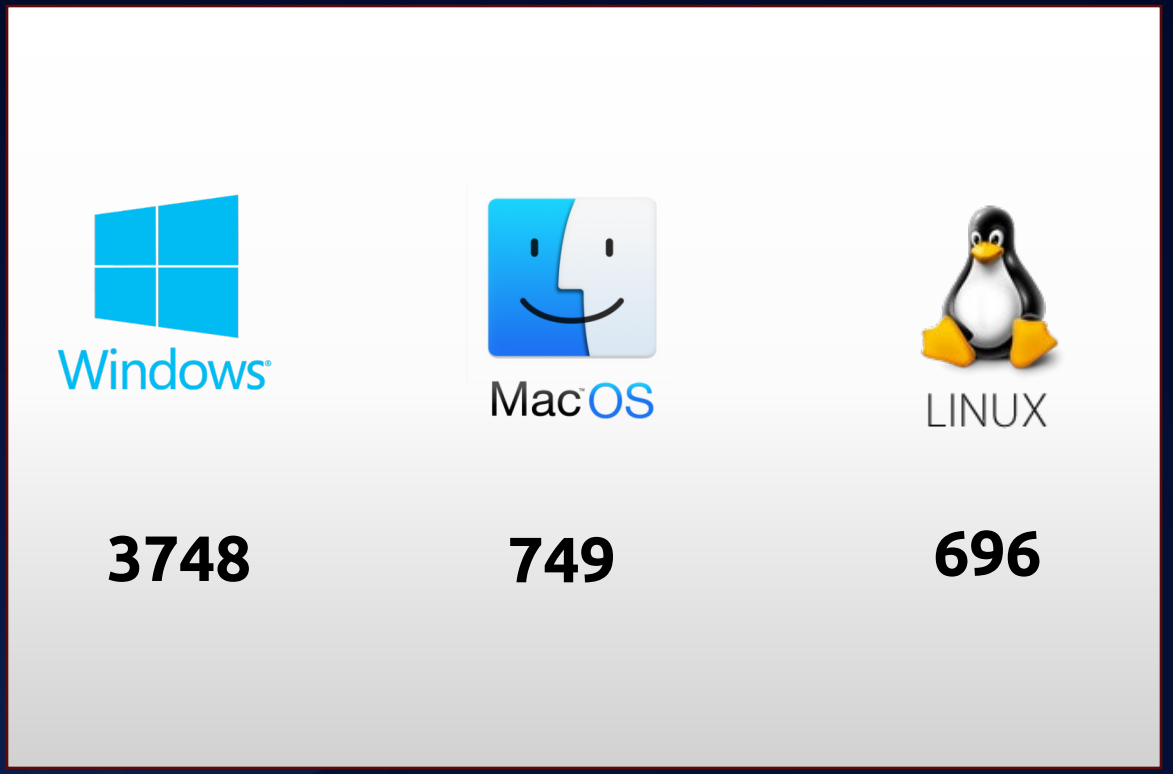
Rule Distribution by Operating Systems

As ADEO MDR Service, we have a total of **5000+** 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: **3748 for Windows operating system, 749 for Linux,** and **696 for MacOS.**

The detection rules we have developed cover approximately **94%** 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 94%** for all our customers across three operating systems and their derivatives.



"We provide support with a detection rate of over 94% for three operating systems and their derivatives for all our customers."

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.

ADEO
CYBER SECURITY

2024 Cyber Security Trends and Predictions

2024 Cyber Security Trends and Predictions

Halil Öztürkci:

As we enter 2024, we are experiencing a period where technology is advancing at a dizzying pace, and digital transformation is deeply impacting every sector. The normalization of remote work models post-pandemic and the increasing demand for cloud-based solutions further elevate the importance of cybersecurity.

We see that cybercriminals are also adapting to these changing conditions, constantly evolving their attack methods. Technologies such as artificial intelligence, machine learning, and automation pose both opportunities and threats in the field of cybersecurity. Regulations regarding data privacy and compliance are gaining momentum worldwide.

In this dynamic environment, it is crucial upon both organizations and individuals to remain vigilant against cyber threats, adopt a proactive approach, and implement best practices. Now, let's take a look together at the main trends and predictions that we believe will shape the cybersecurity agenda in 2024.

Artificial Intelligence (AI) Supported Cybersecurity and Attacks

In 2024, we expect to see the more effective use of artificial intelligence (AI) technology in cybersecurity. AI-based solutions will become more widespread in threat detection, anomaly detection, and incident response. However, the spread of AI also poses a significant risk if it falls into the hands of cybercriminals. Cybercriminals can exploit AI for their own purposes, such as creating deep fake content, conducting social engineering via chatbots, or automating attacks. Therefore, it becomes crucial to develop AI-supported defense mechanisms and train competent experts in this field.

Fighting Against Information Operations

Disinformation campaigns and information operations have been on the rise in recent years. Especially during critical election periods, propaganda activities in cyberspace intensify, involving the spread of false information and manipulation of the public. We anticipate an increase in such operations in various countries before and after elections in 2024 as well. Social media platforms, governments, civil society organizations, and, of course, cybersecurity firms should collaborate in combating disinformation. Developing verification mechanisms, increasing transparency, and enhancing media literacy among users will be key to this effort.

2024 Cyber Security Trends and Predictions

The Evolution of Ransomware

Ransomware attacks continue to be the nightmare of organizations. Attackers not only encrypt data but also threaten to expose victims publicly to demand higher ransoms. In 2024, we anticipate ransomware becoming even more sophisticated, with attackers developing new tactics. For instance, we may see the emergence of AI-based ransomware, attempts to tarnish the reputation of organizations using deep fake technology, and the use of advanced encryption methods. To combat this threat, critical measures such as improving backup and incident response processes, enhancing security awareness, and reducing the attack surface are essential.

New Regulations and Compliance in Data Privacy

Data privacy regulations and compliance will maintain their prominence in 2024. The EU's GDPR has led many countries worldwide to enact similar data protection laws. Next year, we expect more countries to implement comprehensive data privacy regulations. In light of these regulations, organizations will need to increase their compliance efforts and improve their data management processes. Embracing data ethics principles will also become important for companies seeking to preserve customer trust and reputation.

Zero Trust and Identity Management

Increased cyber threats and hybrid work models have revealed the inadequacy of traditional security approaches. Architectures based on the Zero Trust principle will rapidly proliferate in 2024. This model, based on the principle of "never trust, always verify," requires continuous verification of every user, device, and application on the network. In this way, even if an attacker infiltrates the network, the damage can be contained. However, the success of the Zero Trust model depends on a robust identity and access management infrastructure. Therefore, advanced methods such as multi-factor authentication, biometric technologies, and risk-based authentication will come to the forefront.

2024 Cyber Security Trends and Predictions

Supply Chain Attacks and Third-Party Risk Management

As organizations become part of the digital ecosystem, weak links in the supply chain become targets for cybercriminals. Incidents like SolarWinds and Kaseya demonstrated how devastating attacks on software and services that are part of the supply chain can be. In 2024, we anticipate that supply chain attacks will continue to increase. These attacks can impact not only the directly targeted organization but also all stakeholders involved with that organization. Therefore, third-party risk management becomes critically important. Regular assessment of the cybersecurity maturity levels of suppliers and business partners, clear definition of security requirements in contracts, and proactive measures against security vulnerabilities are necessary.

OT and IoT Security

Operational Technology (OT) systems and Internet of Things (IoT) devices are increasingly becoming the focus of cybercriminals. These systems, used in critical sectors such as factories, power plants, and smart city infrastructures, may lack traditional IT security measures. Moreover, many IoT devices harbor security vulnerabilities such as outdated software, default passwords, and weak encryption. In 2024, we expect to see an increase in attacks targeting OT and IoT systems, leading to the development of new regulations and standards in this field. Additionally, there will be a growing demand for solutions such as endpoint security, network segmentation, and secure remote access.

In an environment where cyber threats are constantly changing and evolving, it is important to remember that cybersecurity is not just a technology issue but also a matter of people and processes. For organizations that aim to be successful in 2024, it is essential to increase the cyber awareness of all employees, integrate cybersecurity into business processes, and ensure top management commitment.

Let's not forget that cybersecurity is a shared responsibility for all of us. By working together, we can minimize cyber risks in the digital transformation era and safely leverage the opportunities offered by new technologies.

"With best wishes for a cyber-secure future;
Halil Öztürkci"

2024 Cyber Security Trends and Predictions

What Does ChatGPT Say?

Cybersecurity threats are rapidly evolving and diversifying, but some potential types of attacks could include:

Ransomware Attacks:

These attacks involve malicious software that locks computer systems or files and demands ransom. Particularly, large corporations, healthcare institutions, and public agencies can be targeted.

Cloud-Based Attacks:

As organizations become more dependent on cloud services, the prevalence of cloud-based attacks may increase. This includes attacks where malicious software or data breaches target cloud infrastructure.

Internet of Things (IoT) Attacks:

With the proliferation of IoT devices, attacks carried out through these devices may also increase. For example, IoT devices such as security cameras, thermostats, and smart home devices can be vulnerabilities in a network.

Artificial Intelligence (AI) Supported Attacks:

Artificial intelligence and machine learning can be utilized by cyber attackers to carry out more sophisticated and unpredictable attacks. This could translate into faster and more effective attacks.

Big Data Breaches:

Large enterprises' and organizations' big data storage and analytics systems can be valuable targets for malicious individuals. Such breaches can lead to the leakage or theft of personal data of millions of individuals.

State-Sponsored Cyber Attacks:

Geopolitical tensions between countries can lead to an increase in state-sponsored cyber attacks. Such attacks can target government institutions, infrastructure, or strategic industries.

These are just a few examples, but there are constantly emerging new threats and types of attacks in the field of cybersecurity. Therefore, it is important for organizations to continuously update and improve their security measures.

"The important thing is to continue taking cybersecurity measures and being cautious during your online activities."

2024 Cyber Security Trends and Predictions

What Does Gemini Say?

Cybersecurity threats are rapidly evolving and diversifying, but some possible types of attacks may include:

Expected Threats:

- Artificial intelligence and machine learning-based attacks
- Endpoint attacks
- Cloud security risks
- Cyber espionage
- Social engineering attacks
- IoT attacks
- Attacks on critical infrastructure
- Destructive hacktivism
- Olympic-themed frauds
- Attacks on managed service providers

Ways to Protect:

- Artificial intelligence and machine learning-supported security software
- Being a conscious user
- Staying up to date
- Backup
- Cybersecurity training
- Data protection and privacy policies

Key Points:

- Cyberattacks are becoming more complex and dangerous every day.
- Investing in cybersecurity and staying updated is more important than ever.
- Individuals and organizations need to act consciously against cybersecurity risks.

Recommendations #TOP 5

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.

Artificial Intelligence and Cyber Security

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.

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

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

"Be Prepared for Current Attacks with Picus."

Picus, joining the product family in 2023, enables MDR teams to be proactive against cyber attacks by offering many advantages such as realistic attack simulations, identifying cybersecurity vulnerabilities and weaknesses, increasing awareness and knowledge, providing training and exercise opportunities, and optimizing defense strategies with reporting and analysis. In this way, Picus significantly improves the cyber resilience of MDR teams and helps them become stronger against cyber attacks.

** In our 2023 initiatives, we utilized the Picus product in our testing efforts. We extend our gratitude for this collaboration.*

"Discover, Capture, and Analyze Malware with Threatzone."

Threatzone, malicious software analysis platform that enables you to see the malicious activities of files on computers in an isolated environment. ADEO MDR team detects complex attacks by analyzing files in an isolated environment using Threat Zone Sandbox and ensures quick and secure analysis by eliminating the risk of malicious infection.

"Advanced Endpoint Protection with SentinelOne"

ADEO MDR team provides protection by automatically detecting cyber threats with AI-powered SentinelONE. SentinelONE facilitates rapid response to detected incidents, ensuring the security of your systems.

"Provide Accurate and Timely Intelligence with Cyberthint."

ADEO MDR team quickly accesses detailed and accurate information about cyber threats and attackers with Cyberthint. This enables proactive protection by swiftly identifying and intervening in attacks without delay.

Service Network

Firsts in ADEO and in Turkey

We are on the Top 250 MSSPs List

ADEO Cyber Security achieved a great success by being listed on the "Top 250 MSSPs List," prepared by MSSP Alert, as the "first and only Turkish Cyber Security company".
In 2023, it moved up 47 spots in the rankings.

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

- First Digital Forensics Laboratory, 2015
- Membership in Cyber Security Clustering, 2018
- First Carbon Black MSSP Partner, 2019
- First MDR Services Partner, 2020
- First Palo Alto Networks MSSP Partner, 2020 (Adeo is among the 11 partners worldwide with this capability.)
- First ADTR Service Provider, 2023
- First APTR Service Provider, 2023


ADEO
CYBER SECURITY
ADEO Cyber Security Services
@adeocomtr
ADEOcomtr
@adeocomtr
@adeocomtr
www.adeo.com.tr
GENEL / PUBLIC