VECTRA
SECURITY THAT THINKS.®

CASE STUDY

mLeasing uses the most modern technology based on artificial intelligence to detect and respond to modern cyberattacks

mLeasing, a leading leasing company in Poland and part of the mBank group, was looking for a modern solution that enabled the identification of online threats in real time. Eager to find a modern solution equipped with detection and response, its IT Security team conducted a process to assess and test (POC) solutions available on the market.

"Today it is no trick to be able to identify known threats because that's what everyone can do. The real art and challenge is the ability to detect new and unknown 'zero day' threats that may appear in any, even in the most secured, IT environment," says Marek Jastrzębski, Director of the IT Department of mLeasing Sp. z o.o.

"The Vectra® Cognito® solution, thanks to high levels of automation, minimizes the time needed to detect a threat and allows for an immediate response to stop an attack."

Marek Jastrzębski
Director of the IT Department
mLeasing Sp. z o.o.

Organization

mLeasing Sp. z o. o.

Industry

Financial Services

Challenge

Traditional systems based on signatures or attack patterns only detect threats that are known to the system

Selection criteria

Find a system that would complement the security concept with a state-of-the-art solution based on behavioral analysis, supported by artificial intelligence and deep machine learning

Results

- Automatic evaluation and prioritization performed by Vectra Threat Certainty Index™
- Minimal time needed to detect a threat and ability to immediately respond to an attack
- Detect cyber attacks faster to contain threats more effectively

"Traditional systems based on signatures or attack patterns, in light of contemporary challenges and threats related to cybersecurity, are simply insufficient because they only detect threats that are known to the system," says Jastrzębski. "We were looking for a solution that would complement our security concept with a state-of-the-art solution based on behavioral analysis, assisted by artificial intelligence and deep machine learning. Our goal was to detect hidden cyberattacks faster to more effectively stop threats."

At the conclusion of their evaluations, mLeasing chose Cognito Detect™ and Cognito Detect for Office 365 from Vectra as meeting their requirements to detect and respond to online threats.

Evaluation criteria

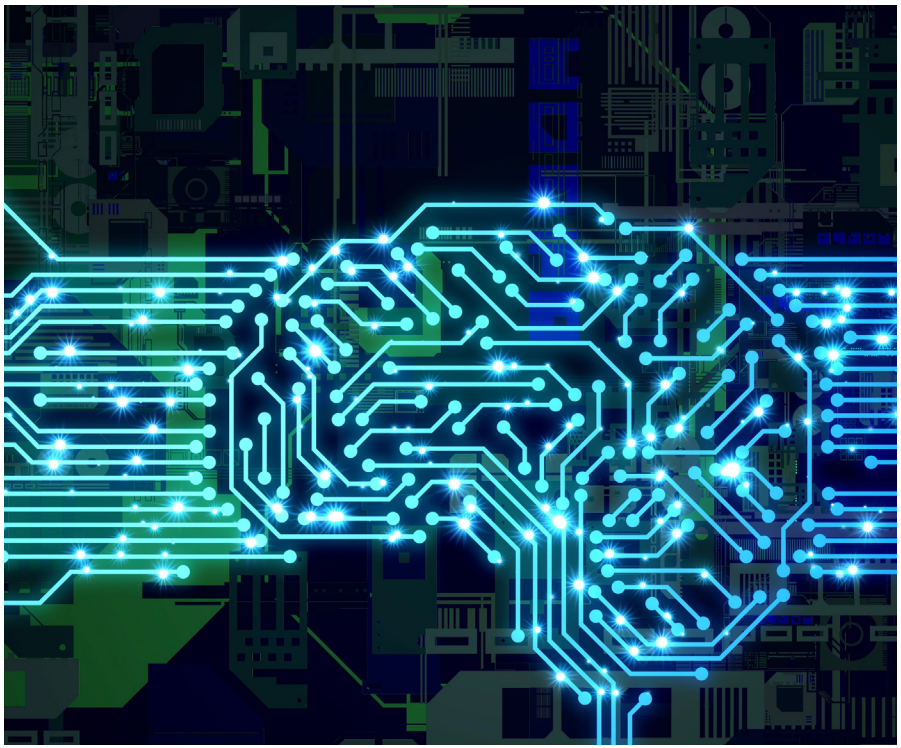
"We realized that the ease of use and automation of Vectra, combined with its high efficiency, will save us time, give us greater understanding of the context of each attack, and facilitate faster reactions to eliminate threats," says Jastrzębski. "Those were the main factors in choosing the Vectra Cognito platform."

The Cognito platform provides full visibility into hidden threats across the entire spectrum of an organization's operation. Through behavioral analysis of the security context-enriched metadata from all network traffic – including data from the cloud, data centers, virtual environments, remote locations, authentication systems, SaaS applications such as Office 365, and all users and IoT devices , leaving attackers with nowhere to hide. The analysis of network metadata is applied to all internal (east-west) traffic, internet-bound (north-south) traffic, the virtual infrastructure, and cloud environments.

"We have all the important information we need on the Cognito Dashboard. Automatic evaluation and prioritization performed by Vectra Threat Certainty Index saves us a lot of time," says Jastrzębski.

"Vectra Threat Certainty Index automatically prioritizes detected threats, so you can easily spot the most critical. The system consolidates hundreds of events and combines them with historical context to identify the host that poses the greatest threat."

Marek Jastrzębski
Director of the IT Department
mLeasing Sp. z o.o.



How it's used

By automating the manual and time-consuming analysis of security events, the Cognito platform significantly reduces the working time and the security analyst's workload. This allows the mLeasing IT security team to stay ahead of attackers and to respond faster and more efficiently to contemporary hidden threats.

Cognito Detect for Office 365 obtains activity logs from multiple services such as Office 365, AWS, Azure, Active Directory, SharePoint, OneDrive, and Exchange. Vectra analyzes logging, creating and manipulating files, configuring mailbox routing and much more. Vectra, using machine learning algorithms based on artificial intelligence, actively detects the behavior related to attacks in these services and reacts accordingly to prevent breaches and prevent data theft.

After the launch of Vectra, mLeasing's IT security team is now working more efficiently with the ability to respond much faster to emerging modern threats.

"Prioritization performed by Vectra Threat Certainty Index saves us a lot of time."

Marek Jastrzębski
Director of the IT Department
mLeasing Sp. z o.o.

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai