WRITTEN BY

DAWID JANKOWSKI
Cybersecurity Competency Center Director
Sii

A CYBER-SECURITY UPGRADE

Every company needs to ensure the security of its data and information systems. The company's clients count on the confidentiality of the sensitive data, contracts and other information provided, whose disclosure could bring harm. Leakage of such data could be catastrophic in its consequences. An additional element that has appeared on the cybersecurity radar in recent years is artificial intelligence. Both cybercriminals and teams protecting organizations are using it more and more.

The detection and processing of security incidents is handled by dedicated units within the organization called SOCs (Security Operations Center). An organization can have an in-house SOC team or use third-party support using a SOC-as-a-Service (SOCaaS). SOC-as-a-Service is a kind of natural evolution of a company's cybersecurity. There are four main benefits of SOCaaS solutions:

1. **Significantly reduced risk of attack.**
   The cybersecurity experts handle each case individually and constantly monitor security systems. The risk of data leakage or production interruption is therefore significantly reduced.

2. **Faster detection and prevention.**
   Time plays a key role during an attack - once a machine is infected, it must be immediately isolated from the rest, whereas once the user account is hijacked, the password must be immediately reset.

3. **Scalability.**
   As an organization grows, the SOCaaS grows with it. For a SOCaaS provider like Sii, doubling the SOC is not a problem as we have a vast number of experts ready to work 24/7.

4. **Lower costs.**
   SOCaaS eliminates the need to maintain an in-house unit, including: staff, employee training, office, hardware or licenses. It is estimated that with optimal calibration, SOCaaS can cost up to 90% less than a traditional in-house SOC unit.

USING AI IN THE SECURITY INCIDENT MANAGEMENT PROCESS

It is crucial for an organization to quickly detect and disrupt an ongoing attack. The sooner a threat is detected and resolved, the lower the impact on the organization and the potential expenses. Safety breaches in organizations with fully implemented AI and automation in the security area cost 65% less than breaches in organizations without such solutions.

INCIDENT DETECTION

In order to effectively block an attack on an organization, we must first detect such an attack or attempted attack. It is rarely a single incident - most often the attack consists of a series of interrelated actions enabling the attacker to achieve their goal.

Here are a few specific examples of how successful implementation of cloud-based and AI-supported solutions reduces the problems that are present in the classic solution:

HANDLING ATTACKS WITH UNKNOWN SIGNATURES

If you rely only on known signatures and simple behavior patterns, there is a high risk that a non-standard attack, or a zero-day attack, will go undetected.

Solution: Machine Learning (ML) is most suitable for solving complex problems by observing incoming data and identifying trends that are not immediately obvious.

> Both cybercriminals and teams protecting organizations are using artificial intelligence more and more.

HANDLING USER-DIRECTED ATTACKS

The classic solution is only capable of recognizing user-directed attacks to a limited extent.

Solution: Using ML algorithms helps us determine the standard behavior of individual users and detect anomalies. While it is relatively easy to steal someone's username and password using, for instance, social engineering, impersonating that person by mimicking their behavior is much more difficult.

ALARM FATIGUE

Traditional solutions can generate a large number of false alarms. A large number of irrelevant or false alarms leads to analyst fatigue, which is the most common cause of errors and disregard for real threats in incident handling.

Solution: A SIEM platform with built-in machine learning models enables accurate detection and pre-verification of real threats among the millions of incidents generated.

HANDLING SECURITY INCIDENTS

Another key part of the process is responding to security incidents, which involves the vast majority of tasks performed by SOC analysts. Our first thought when thinking about AI in the context of incident response is the complete automation of the process. We can imagine a system in which SOC analysts are no longer needed. The reality is somewhat different - while AI is used to automate more typical tasks, its main role is to support the SOC analyst in decision-making. At that point, we speak of Intelligence Amplification (IA).

The following are examples of activities supported by Artificial Intelligence in the area of cybersecurity.

Data suggestion - when responding to an incident, the SOC analyst uses logs from various systems. This is a very time-consuming process. AI already searches and retrieves the necessary data during incident creation.

Risk identification and incident prioritization - one of the analyst's first tasks is the so-called triage. The analyst identifies the risk, verifies the affected systems and determines the type of threat. ML algorithms based on available data and previous incidents make it possible to automate this step.

Automation of containment activities - the goal of containment actions is to limit the damage caused by the current security incident. There is a risk of an incident being addressed too late for the analyst to effectively resolve it. This is where AI comes to the rescue. Once a high probability of an intrusion is identified, the necessary actions (e.g., account lockouts) are executed automatically.

RECOMMENDATIONS

Machine learning algorithms can suggest required actions in handling certain types of incidents. This is a particularly useful feature for reducing response times and improving response quality.

All of the features and advantages of SOC-as-a-Service, as well as the ways in which AI streamlines and automates the work of security analysts, allow us to conclude that this method of monitoring and handling security incidents is an optimal solution for all institutions for which security is important, but is not their main area of activity. We have a large team of certified specialists and experience in providing this type of service for large financial institutions in Poland and around the world.