Infosys®
Navigate your next

VIEWPOINT

THE FUTURE OF TOMORROW: AUTOMATION FOR CYBERSECURITY

Artificial intelligence can improve security by automating and speeding up threat detection and response. For this reason, security orchestration, automation and response, or SOAR, technology solutions are becoming a must-have tool in the arsenal of security operation teams. Here's how it works.

Infosys® | Knowledge Institute

The future of tomorrow: automation for cybersecurity

In today's technology-driven world, cyberattacks are no longer the exception; they are the rule. Driven by digital transformation, businesses increasingly implement more IT infrastructure. This increases the size of their corporate attack surface. At the same time, hackers take advantage of new technologies, coming up with new solutions for their offensive strategies.

Automated password-cracking programs, AI-powered botnets and automated phishing are just a few ways hackers can use automation, artificial intelligence and machine learning to their advantage. Sophisticated cyberattacks and constant cyber arms races put businesses under threat more than ever.

The need to extend human capabilities

Hackers use automated tools to penetrate corporate networks quickly and precisely. Take for example an AI-powered DDoS attack. To conduct any sort of online business, an enterprise needs to have access to the internet. Stable functioning of a company's operation resources is becoming a critical condition for users and partners around the world.

A DDoS, or denial-of-service, attack is a massive flood of requests from a huge number of infected devices such as computers, mobile phones and servers. The main focus is to exhaust network resources and equipment, security tools, computing resources, and applications. Once such a server has been filled with these false requests, it will no longer respond to normal traffic, thus denying legitimate users access to the web application. Attackers actively use DDoS attacks for extortion and to launch competitive wars. The consequences of a DDoS attack can be devastating in terms of loss of market share, profits and reputation.

With artificial intelligence, hackers can unleash more powerful DDoS attacks. A machine can produce an unlimited number of requests. It does not tire or lose concentration. Stopping the attack requires a sophisticated filtering system to block the malicious traffic. The AI-powered DDoS attacks can maintain constant momentum and continue operating even if under pressure from defense mechanisms.[1]

Cybersecurity practitioners on the ground receive lots of logs and data. They identify the issues, but then it becomes difficult to evaluate the meaning of threats, what they affect and which patterns they create. Many different tasks overwhelm the analysts. On top of that, a current shortage of almost 3 million security specialists globally makes it difficult to keep up with constantly evolving cybersecurity tools.[2] Apart from the need for constant learning and upskilling, the analysts waste a lot of time manually entering large amounts of data into systems. This can cause operational inefficiencies and waste critical time.

Standard security equipment can automatically prevent only previously known attacks, and its response to the threats that exist today is as ineffective as using swords to fight machine guns. Human analysts simply cannot predict unknown incidents and can work only with their knowledge of attacks that have already occurred. While the analysts are still figuring out what has happened, the hackers could gain a foothold in the system and destroy the traces of their own penetration. So how can businesses manage risks and respond to incidents in a cost-effective manner?

> Artificial intelligence coupled with machine learning can tackle cyberthreats before they prove disastrous

Security Orchestration, Automation and Response

SOAR solutions are being evaluated by security operations leaders as a key tool to organize and automate investigation and response processes.[3] According to Gartner, SOAR is a set of "technologies that enable organizations to take inputs from a variety of sources (mostly from security information and event management [SIEM] systems) and apply workflows aligned to processes and procedures."

A fairly large part of the SOAR functionality belongs to the SIEM class. Therefore, SOAR solutions either include the SIEM module as an element of the initial collection and processing of information about incidents, or integrate with external SIEMs to receive alarms, attack vectors, signs of compromise and other characteristics of malicious activity.

SOAR is a set of technology features that goes beyond producing recommendations. It automatically responds to events. SOAR's functions include orchestration, automation and response.

Orchestration

Orchestration coordinates the integration of security measures with an enterprise's information systems. It combines and coordinates the workflows with manual and automated steps. During an investigation, an analyst interacts with information systems and information technology to gain the context and to collect data. The process is very monotonous and significantly slows down the investigation. Orchestration allows integration with third-party systems for data collection and management. This reduces spending time on switching between different consoles and interfaces. For example, when an attack is detected, the orchestration starts the additional processes that check indicators of compromise. It then launches the search for malicious codes.

Automation

A SOAR solution describes and automates the actions that are carried out as part of the investigation through prepared response plans, also known as a playbook. Automation occurs through describing beforehand the steps and processes of investigation, detecting incidents, and reacting to them with the help of orchestration. Gartner defines automation as the concept that "involve[s] the capability of software and systems to execute functions on their own, typically to affect other information systems and applications."[3] The system automates the actions of the same type that analysts had previously performed manually.

This significantly reduces the time to investigate and collect the necessary

data required to make a decision. Some processes require a human to make a final decision. The system stops the process and waits for further instructions from the analyst. Take for example identity access management. After the system automatically collects the incident data, the analyst examines the evidence and decides whether to lock a user account or move the host to an isolated segment. This playbook allows the user to build complex structures with different development paths and branches, depending on the result of an analysis.

Response

Through orchestration, the SOAR solution has the ability to automatically respond to identified incidents. SOAR collects more detailed statistics and limits potentially dangerous operations. Ransomware infections demonstrate the need for a timely response to minimize the spread of malicious codes.

The damage from a ransom attack depends greatly on the speed of reaction. When automated scripts detect compromised devices using indicators of compromise, response tools disconnect them from the main network and thus block the further spread of malicious code.

Case study : LockerGoga ' 19 Ransom

In 2019, ransomware remains successful and profitable because it provides immediate financial returns. Ransom attacks are a common type of cyberattack that encrypt a company's systems and data and demand money in cryptocurrency. Once the victim pays, the criminals release a decryption key and the company can start the recovery process. Cybercriminals don't need to sell stolen information to make money, as the victim pays directly. On top of that, digital currency provides an easy way to monetize ransomware. Cryptocurrency eliminates the need for illegal money transfers from victims' accounts, money mules or middlemen.

Today, ransomware is becoming more tailored and targeted. There is a new type of ransomware known as LockerGoga. The ransom targets and attacks the manufacturing and industrial sectors. In March 2019, it hit Norsk Hydro, a global Norwegian aluminum company.[4] The attack partially disrupted the company's production operations in 160 of its plants in 40 countries. The company had to switch to manual operations and to prevent 35,000 employees from logging in to their computers. Norsk Hydro refused to pay and was able to restore its operations back to normal. The company had a good level of cyber protection and had a secured, uncompromised backup of its system in place. However, the business still suffered the costs of the breach, which amounted to between US$ 35,000,000 and US$ 41,000,000 during the first week. The investigation of the case showed that the threat actors delivered the malware by phishing. Today phishing is the most popular method of distributing ransomware.

Types of SOAR tools

There are three main types of SOAR tools: security orchestration and automation (SOA), security incident and response platforms (SIRPs), and threat intelligence platforms (TIPs). SOA provides orchestration and automation of security management processes. SIRPs respond to incidents and restores operation systems back to normal after an attack. The TIPs are interactive investigation platforms that provide intelligent event processing for monitoring information security systems. All platforms integrate with each other, and as a whole make up SOAR, with the most efficient implementation of all functions.

Other important SOAR functions are performance assessment, information security incident management and integration with threat intelligence providers. For example, a SOAR solution can become a single point of information for security incident management in a company.

The future of SOAR technologies

By the end of 2022, 30% of such organizations will leverage SOAR tools, compared with 5% now.[3]

AI-powered solutions are imperative in today's world to fight cybercriminals. Artificial intelligence develops unique insights that humans cannot. The implementation of artificial intelligence and automation of cybersecurity processes improve the overall efficiency and effectiveness of existing protection. SOAR solutions cannot replace the SOC team completely. Rather, they extend human capabilities. The benefits include increased speed of detection and flagging of anomalies, thorough risk analysis, and incident investigation.

Artificial intelligence produces algorithms that help identify physical and logical threats. It can reconfigure devices to defend themselves, fix bugs in the codes and correct vulnerabilities. With the use of machine learning, artificial intelligence can contain threats before they get a chance to spread to the entire system and infiltrate it.

Although the SOAR market is quite young, it is now clear that effective response to information security incidents will require tools to automate these processes.

References

1. "The Rise of Artificial Intelligence DDoS attacks," Network World, 2019, https://www.networkworld.com/article/3289108/the-rise-of-artificial-intelligence-ddos-attacks.html
2. "Artificial Intelligence: A Tool or a Threat to Cybersecurity?" Readwrite, 2019, https://readwrite.com/2019/08/21/artificial-intelligence-a-tool-or-a-threat-to-cybersecurity/
3. "Market Guide for Security Orchestration, Automation and Response Solutions," Gartner, 2019, https://www.gartner.com/doc/reprints?id=1-13JT7BOP&ct=190703&st=sb
4. "The LockerGoga Ransomware Attack: A worst-case scenario for industrial operations," AXA XL, 2019, https://axaxl.com/fast-fast-forward/articles/the-locker-goga-ransomware-attack_a-worst-case-scenario-for-industrial-operations

SME

Vishwanath Nagaraj

Industry Principal – Cybersecurity
Vishwanath.Nagaraj@infosys.com

Author

Yulia De Bari

Consultant – Infosys Knowledge Institute
Yulia.Debari@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next