Exploring the Impact of **SOAR** on Cybersecurity Operations

Whitepaper

2023

AGILEBLUE

WHAT IS SOAR?

Security Orchestration, Automation and Response (SOAR)

SOAR is a revolutionary approach for organizations to protect their assets better and to respond quickly against cyber-attacks. Coined by Gartner when it first burst onto the scene in 2015, this innovative technology combines Security Orchestration, Automation & Response (SOAR) with security incident response platforms (SIRP) and threat intelligence platforms (TIPs). By introducing automated responses to incidents, IT teams can gain back valuable time while also having the ability to closely observe potential threats in order to prevent them from occurring again. As a whole, SOAR provides a holistic threat management approach that includes managing threats and vulnerabilities, responding to security incidents, and automating security operations. SOAR has become pivotal in modern SOC as it has transformed cybersecurity by streamlining incident response and increasing efficiency for IT teams.

SOAR: THE SOLUTION TO MANY SECURITY CHALLENGES

The cyber security landscape is shifting, and with it comes increased risk. Modern teams are facing a barrage of technological complexity that brings significant pressure in the form of abundant alert volumes combined with limited experts and resources to handle them effectively. This reality only intensifies as new IT advancements like OT, Blockchain, Cloud, and more require additional oversight for effective defense strategies - exacerbating an already challenging situation for security teams.

SECURITY CHALLENGES

01 Growing Complexity and Volume of Threats

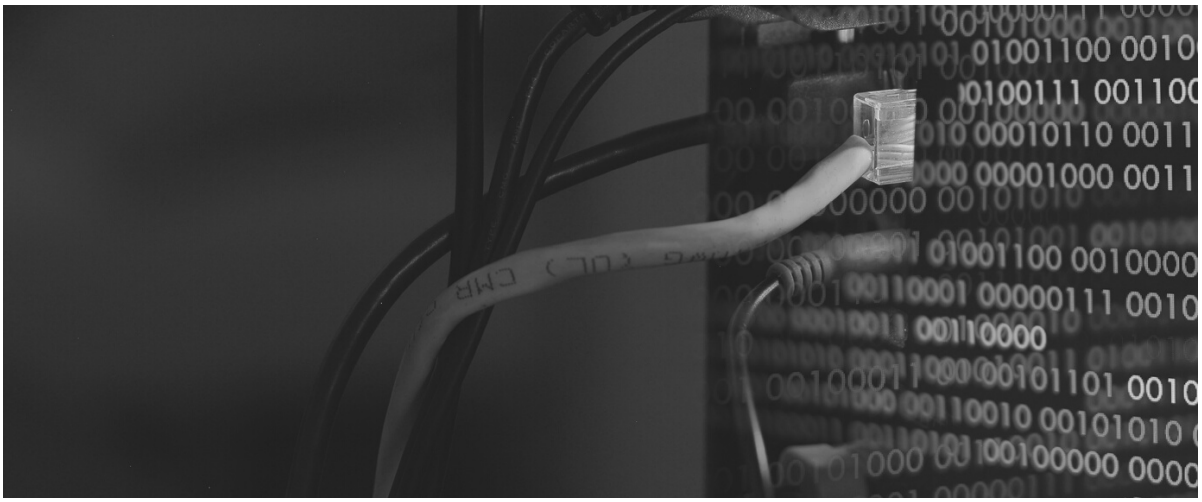
As technology in the world of cybersecurity takes a step forward in innovation, so do cybercriminals. For example, while in the world of cybersecurity, artificial intelligence (AI) has vastly improved how we are able to discover and respond to cyber threats, cybercriminals have begun to leverage and weaponize AI-based technology for their own attacks. According to SecurityScorecard, here are the ways we know that hackers have begun exploiting AI:

- AI algorithms being altered to create undetectable attacks such as phishing
- Data poisoning of AI training data sets leading to incorrect data being presented and affecting the accuracy of an organization's system
- Input attacks involving malicious codes being set off at a specific time, even months after altering the code, to maximize attack impact
- Cybercriminals using AI technologies to develop malware capable of mimicking trusted systems and executing undetectable ransomware attacks

Not only are attacks gaining sophistication, but the threat landscape for all organizations is also continually expanding. According to UpGuard, some of the reasons are:

- Greater dependence on software as a service (SaaS) products
- Networks on the dark web that enable cybercriminals to post data for sale
- External factors, such as the shift to remote work due to the COVID-19 pandemic
- Faster software releases with added functions
- Hardware developments, such as internet of things (IoT) devices
- Previously mentioned technological advancements leading to more sophisticated attack methods

In 2022 ransomware attacks proved to be a constant threat facing all sectors and organizations. Kaspersky Lab reported that in 2022, the percentage of users impacted by ransomware doubled within the first 10 months. Furthermore, phishing attacks increased by a staggering 61% in 2022, with over 3 million successful phishing attacks in the third quarter alone, according to SlashNext's "2022 State of Phishing" report. Unfortunately, this momentum of increasing attacks year over year will only continue on the same path upwards. According to TechTarget, it is estimated that cybercriminals will steal 33 billion records in 2023, which is a 175% increase since 2018.



02 Increased Complexity of Business IT Infrastructure

The SolarWinds IT Trends Report 2022 has found that complexity continues to be a major challenge for IT teams, and their ability to support the bottom line of businesses is being severely hampered. This increased demand from multiple departments across new tools, technologies, and fragmentation between legacy models only heighten this problem - with only 16% of respondents feeling extremely confident in managing these complex environments. It's an issue compounded by over one-third admitting they're not fully prepared for it yet.

The attack surface for most organizations has grown significantly in the past ten years. Not only do we now have multiple ways to access and interact with those external internet-facing assets, but due to the ubiquity of mobile devices and cloud computing, the attack surface can be much larger than ever before. This creates additional risks from anomalies that originate outside traditional boundaries. Assets can be exposed through cloud adoption and migrations, and development teams for testing may introduce new assets. Additionally, new netblocks or advertisements may be configured in networks, and subdomains for landing pages hosted by design companies may be created by marketing. To minimize the risk of attack surface area exposure, monitoring various activities such as sales and marketing campaigns, e-commerce activities, IT operations configuration changes, patching services, and security fixes are important. Mergers and acquisitions may also bring new assets that require a risk assessment, while uncontrolled external elements in a business's network infrastructure framework must not be ignored, as they can represent an attack vector opportunity if left unmonitored. Third-party hosting providers are often used to provide additional resources, making supply chain risk management essential.

03 Alert Fatigue

IT professionals can be inundated with a high volume of alerts on any given day, which may often lead to alert fatigue – the failure to prioritize and respond in a timely fashion. Alert neglect carries serious consequences, such as system failures, data breaches, or network downtime. Yet, there are so many false alarms that it becomes difficult for IT personnel to decide which one deserves immediate action. Aside from creating dangerous scenarios where critical issues go unresolved, this overload also trends toward burnout among tech teams because care must be taken when addressing these increasing volumes of notifications.

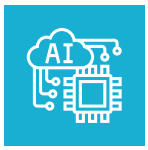
04 Shortage of Skills

Organizations around the globe are struggling to find qualified cybersecurity professionals as demand for these experts continues to outpace supply. Unfortunately, inadequate education and training opportunities make it difficult for individuals seeking entry into this field without prior experience or knowledge in cybersecurity. The unpredictable nature of cyber threats further complicates matters, requiring continuous learning - something that is both time-consuming and resource intensive. As such, the industry faces a formidable challenge of finding sufficient talent with strong expertise in protecting against data breaches and other types of malicious attacks on their networks.

According to (ISC)2's 2022 workforce study, the global cybersecurity workforce has expanded to a record-high of 4.7 million individuals, which is a positive development. Nonetheless, the study also reveals that there is still a demand for over 3.4 million security professionals, representing an increase of more than 26% from the previous year.

UNLOCKING THE BENEFITS OF SOAR

Fortunately, security engineers possess a problem-solving mindset. As a result of their drive to create a solution that would enhance analysts' effectiveness in combating complex cyber threats while simplifying their workload, they developed SOAR. Here is how SOAR addresses the most pressing cybersecurity concerns:



Tackling Weaponized AI

SOAR is an essential tool in defending against weaponized artificial intelligence (AI). Weaponized AI uses AI-powered technology to perform malicious activities such as malware injection or social engineering attacks. By leveraging machine learning algorithms, attackers can create sophisticated attack vectors that are challenging to detect and mitigate using traditional security measures. SOAR can help organizations defend against weaponized AI by automating incident response and remediation workflows, reducing the time it takes to detect and respond to attacks. Additionally, SOAR platforms can integrate with threat intelligence feeds, enabling the system to identify and respond to known attack patterns automatically. This integration also allows for identifying new and emerging threats, enabling security teams to proactively develop new response workflows and mitigate the threat before it can cause significant damage. Overall, SOAR is an essential tool in combating weaponized AI and can help organizations enhance their overall security posture in the face of this evolving threat landscape.

Overcoming False Positives

To solve the issue of false positives, SOAR relies on its advanced automation capabilities to determine which alerts have previously been marked as false positives by security experts. With this information, the system can independently differentiate between genuine threats and false positives, improving the accuracy of the alert detection process.

Cybersecurity Talent Gap

The shortage of skilled security professionals is a significant challenge for the industry, as the demand for these experts far exceeds the current supply. However, SOAR can assist SOC teams in overcoming this issue by automating a significant portion of their security operations, reducing the need to hire additional security professionals to manage the expanding workload. This capability enables organizations to achieve greater efficiency and productivity in their security operations without relying solely on increasing headcount.

Growing Complex Cyber Threats

To address the issue of sophisticated cyber threats, Cloud SOAR leverages its machine learning engine to assist security experts in making informed and strategic decisions regarding mitigating cyber threats. Additionally, Cloud SOAR utilizes advanced automation capabilities to learn and recognize the attributes of incoming threats, providing actionable recommendations when a similar threat is detected in the future.

Flexibility and Ease of Integration

SOAR platforms are designed to provide a flexible and integrated approach to managing security operations. One of the key benefits of SOAR is its flexibility, which allows organizations to customize the platform to meet their unique security needs. With SOAR, security teams can easily integrate various security tools, such as firewalls, intrusion detection systems, and endpoint protection systems, into a single platform. This integration allows for streamlined security operations, improved response times, and increased efficiency.

Security Orchestration, Automation, and Response are the Future of Cybersecurity

According to Markets and Markets, in 2022, the SOAR market was valued at an estimated USD $1.1 billion and is expected to reach USD $2.3 billion by 2027. This is no surprise, as SOAR has become pivotal in modern SOC.

Security Orchestration, Automation, and Response (SOAR) has emerged as a solution for security teams to address the continuously evolving cybersecurity challenges. As cyber criminals are already leveraging automation to execute unpredictable attacks, it is logical to utilize advanced security technologies to counter them.

AGILEBLUE

WE'RE HERE TO HELP.

Uncover the complete story behind your cybersecurity incidents. AgileBlue's security orchestration, automation and response (SOAR) solution provides your organization with intelligent machine learning capabilities to automate mundane tasks in order to free up team time - all while offering comprehensive protection of networks, data & infrastructure, to gain smart insights that reveal a full picture of an incident.

AgileBlue's platform applies intelligent, advanced logic to show a complete story of an incident in a single view. Your team, network, and data deserve insightful and constant protection. This job is never done, but we've got it handled.

For more information on our SOAR solution, visit us at AgileBlue.com.

Ready to start protecting your company?

REQUEST A DEMO