The Post-SOAR Era:

Revolutionizing SecOps with AI-Powered Platforms

Whitepaper

2025

AGILEBLUE

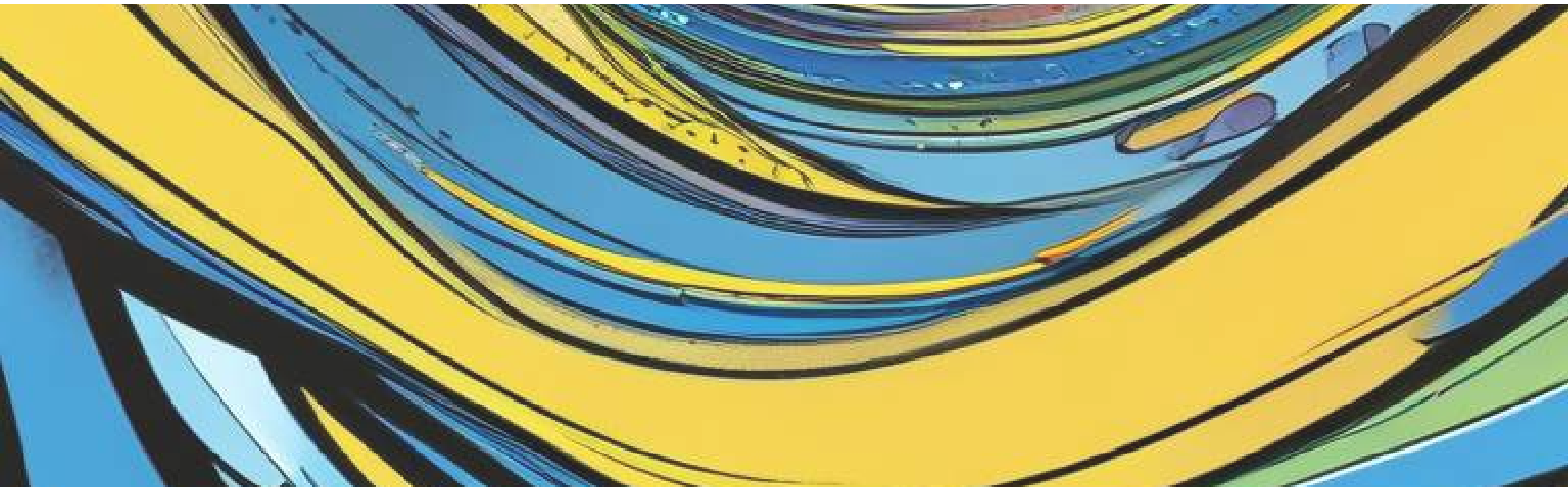
Introduction

The field of cybersecurity has long been a battleground of innovation and adaptation. In 2017, analysts at Gartner coined the term “SOAR”—Security Orchestration, Automation, and Response—to define an emerging class of security tools designed to enhance the efficiency of Security Operations Centers (SOCs). SOAR promised to revolutionize incident response by enabling SOCs to codify their procedures into digitized playbooks. These playbooks integrated and executed tasks across multiple security tools, automating actions that previously required tedious manual effort from human incident responders.

By automating manual processes, SOAR aimed to transform the way organizations managed security operations, offering improved speed and consistency in responding to threats. However, despite these early promises, Gartner later declared SOAR obsolete before its plateau.

Two primary factors contributed to this assessment: the high total cost of ownership and the emergence of competing automation features in other platforms. Compounding this shift, 74% of IT security professionals now report that their organizations are suffering significant impacts from AI-powered threats, highlighting the limitations of static systems in countering today’s advanced adversaries.

This whitepaper explores why SOAR has failed to fulfill its potential in modern security environments and how AI-powered solutions are redefining the future of security operations. As the cybersecurity landscape continues to grow in complexity, organizations require solutions that can dynamically adapt to threats, scale effortlessly, and provide actionable intelligence without the overhead of static, outdated technologies. This is where the post-SOAR era begins, driven by innovations that replace traditional playbooks with real-time, autonomous decision-making capabilities.



The Decline of SOAR

The decline of SOAR is emblematic of a broader shift in cybersecurity technology. Initially introduced to streamline and automate the work of Security Operations Centers (SOCs), SOAR systems struggled to keep up with the growing complexity of cyber threats and organizational infrastructures. Their dependence on static processes, combined with high implementation costs, positioned them as less adaptable to rapidly changing environments. In fact, organizations that integrate AI into their cybersecurity prevention solutions save an average of USD 2.2 million in breach costs.

Integration Challenges in Modern IT Environments

While SOAR systems introduced the concept of integrating multiple security tools, their rigid architectures struggle to keep pace with the complexities of modern IT ecosystems. Multi-cloud and hybrid infrastructures demand dynamic and seamless connectivity across platforms, yet SOAR often requires extensive customization to establish these integrations. This lack of flexibility results in inefficiencies and delays, particularly when handling new or evolving tools within an organization's infrastructure.

Static playbooks further compound this issue, as they rely on predefined workflows that cannot adjust to unexpected or novel attack strategies. As a result, SOAR lacks the agility needed to address the sophisticated and adaptive threats that characterize today's cybersecurity landscape.

Scalability and Threat Adaptability Constraints

The exponential growth in security data and alerts has exposed SOAR's scalability limitations. Designed for simpler environments, these systems often struggle to process and prioritize large volumes of data in real-time. This creates bottlenecks in critical workflows, where even minor delays can provide attackers with opportunities to exploit vulnerabilities. SOAR's reliance on static automation makes it ill-suited to counter dynamic, AI-driven threats. Adversaries are increasingly leveraging machine learning to adjust their tactics mid-attack, while SOAR systems remain confined to fixed response patterns. This inability to adapt in real-time leaves organizations vulnerable to advanced attack strategies.

The shortcomings of SOAR underscore the need for next-generation security solutions. AI-powered solutions offer the scalability, adaptability, and intelligence required to meet the challenges of modern cybersecurity, paving the way for a new era of security operations.

Comparative Analysis: SOAR vs. AI-Powered Security Operations

Feature	Legacy SOAR	AI-Powered SecOps Platform
Accessibility	Limited to only those with technical expertise	Democratizes access to advanced automation
Accuracy	Limited by static rules and manual configurations, leading to potential errors	Continuously learns and refines threat models, achieving higher accuracy over time
Automation Capability	Automates routine tasks	Automates complex tasks and adapts to new threats
Cost-Effectiveness	High initial and maintenance costs	More cost-effective in the long run with less manual intervention
Human Interaction	Dependent on highly skilled analysts	Complements human analysts by helping them to focus on strategic tasks
Integration	Rigid architecture; challenges integrating with modern, dynamic infrastructures	Flexible and adaptive; seamlessly integrates with diverse, evolving infrastructures
Scalability	Struggles with large-scale, multi-cloud environments; requires significant customization	Easily scales across multi-cloud and hybrid environments with minimal configuration
Speed	Dependent on predefined workflows; slower when scaling to large datasets	Processes data in real-time using advanced algorithms for faster detection and response

AI-Powered Threat Defense

AI-powered SecOps platforms revolutionize the way organizations defend against a wide array of cyber threats. Unlike legacy SOAR systems that rely on static playbooks and predefined rules, AI-powered solutions adapt dynamically to each type of attack, providing faster, more accurate, and context-aware responses. Here's how AI-powered systems outperform SOAR in combating different types of cyber attacks:

Malware and Ransomware

SOAR systems often rely on signature-based detection, which struggles with new or evolving malware. AI-powered platforms analyze behavior and detect anomalies, such as unusual file encryption or lateral movement, enabling earlier and more accurate detection of threats like ransomware.

Phishing and Social Engineering

Phishing attacks exploit human errors, making them hard for SOAR systems to detect. With 40% of all phishing emails targeting businesses now generated by AI, traditional tools struggle to keep pace. AI-powered platforms use natural language processing (NLP) to scan communication patterns and identify suspicious emails or links crafted by AI. They also monitor login behavior to detect unusual access attempts, significantly reducing the success of phishing campaigns.

Advanced Persistent Threats (APTs)

APTs are stealthy attacks designed for prolonged infiltration. SOAR systems typically lack the contextual depth needed to uncover such threats. AI-powered platforms correlate data across networks and endpoints to detect anomalies like persistent connections to external servers, disrupting APTs before significant damage occurs.

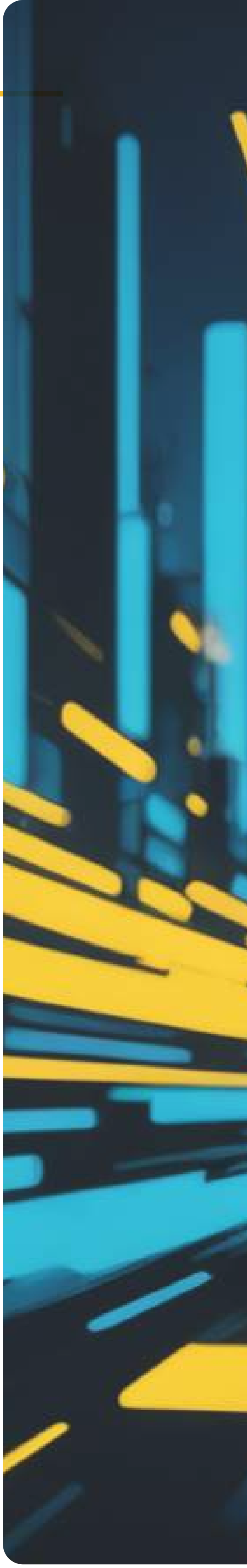
Distributed Denial of Service (DDoS) Attacks

DDoS attacks flood systems with excessive traffic. Legacy SOAR platforms often require manual adjustments to counteract these threats. AI-powered platforms dynamically analyze traffic patterns to distinguish malicious activity from legitimate usage, mitigating DDoS attacks in real-time.

Zero-Day Exploits

Zero-day exploits target unknown vulnerabilities, making them difficult for traditional systems like SOAR to detect due to the absence of signatures or predefined rules. AI-powered platforms excel at identifying these threats by analyzing deviations in code behavior, system interactions, and network activity.

Key Components of an AI-Powered SecOps Solution



Predictive & Real-Time Threat Detection

Combines predictive and real-time monitoring to identify vulnerabilities, anticipate breaches, and respond to threats within milliseconds.

Behavioral Analytics & Adaptive Learning

Applies advanced AI models to establish behavior baselines and dynamically adapts to detect insider threats and sophisticated attack patterns in real-time.

Automation of Repetitive Tasks

Leverages AI to handle tasks such as alert triage, log parsing, and rule updates, enhancing operational efficiency and significantly reducing response times.

Dynamic Playbook Execution

Deploys intelligent and adaptive workflows that adjust in real-time to the context of an incident, ensuring precise and effective responses.

Data Aggregation and Threat Prioritization

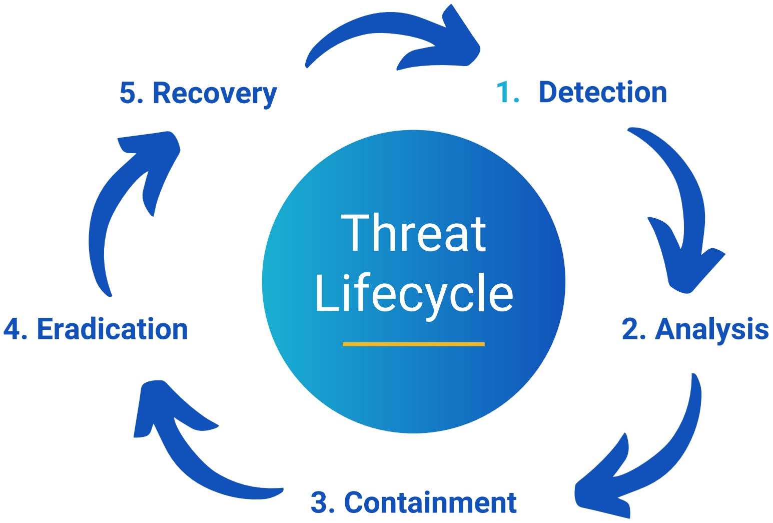
Analyzes and correlates vast amounts of data from multiple sources to detect anomalies and prioritize high-risk threats for immediate action.

Seamless Integration with Existing Tools

Provides unified visibility by integrating with existing security tools, streamlining workflows and enabling cohesive security operations.

AI-Enhanced Threat Lifecycle Management

As cybersecurity threats become increasingly sophisticated, traditional tools like SOAR are struggling to keep pace. AI-powered technologies represent the future of security operations, offering dynamic and powerful capabilities that revolutionize every stage of the threat lifecycle. By comparing the traditional SOAR lifecycle to an AI-powered SecOps lifecycle, the advantages of replacing SOAR with advanced solutions that utilize AI become evident.



SOAR Threat Lifecycle

1. Relies on predefined rules and signatures, limiting its ability to identify novel or evolving threats.
2. Aggregates and correlates data manually or with static playbooks, often lacking context and delaying insights.
3. Uses static workflows to isolate affected systems, which may struggle with complex or dynamic attacks.
4. Executes pre-configured scripts to remove threats but depends on human oversight and limited learning.
5. Restores systems using fixed workflows with minimal integration of lessons learned for future improvements.

AI-Powered Solution Threat Lifecycle

1. Uses anomaly detection and machine learning to identify threats based on behavior, including unknown attack patterns.
2. Employs NLP and data correlation to autonomously identify root causes and impacts, providing actionable insights faster.
3. Dynamically adjusts responses using adaptive playbooks and reinforcement learning to isolate threats effectively.
4. Automatically executes tailored actions like neutralizing malware, refining future responses based on continuous monitoring.
5. Leverages AI-driven insights to identify exploited vulnerabilities and update workflows, improving resilience to future threats.

Introducing Sapphire AI Insights:
SOAR’s Upgraded Replacement

At AgileBlue, innovation and efficiency drive everything we create, and Sapphire AI Insights embodies this vision by redefining organizations’ cybersecurity. AgileBlue's Sapphire AI Insights represents a transformative leap in security operations, replacing outdated static playbooks and rigid workflows with intelligent, adaptive systems. By harnessing the power of machine learning and contextual awareness, Sapphire AI Insights redefines how organizations, respond to and recover from cyberthreats.

Its proactive, flexible approach ensures security teams are always prepared to handle emerging challenges effectively. Sapphire AI Insights stands out for its ability to go beyond automation, offering dynamic capabilities that respond to the complexity of modern cyberattacks. It simplifies operations while strengthening defenses, making it a game-changing solution for organizations seeking to stay ahead of increasingly sophisticated adversaries.

Advanced Features and Capabilities

At the core of Sapphire AI Insights is its ability to merge machine learning with real-time analytics to deliver unparalleled precision in threat detection and response. Sapphire AI, the powerhouse behind the Cerulean AI platform, provides advanced, actionable decision making that significantly expedites response times. By achieving 90% automation of Level 1 and Level 2 triage and decision-making for SOC analysts, Sapphire AI drastically reduces false positives and alleviates the burden of alert fatigue, enabling security teams to focus on critical threats.

Dynamic playbooks are another standout feature, adapting in real-time to the specific characteristics of a given threat. Whether it’s neutralizing a malware attack or isolating a compromised endpoint, Sapphire AI ensures responses are tailored, timely, and effective. By automating these complex processes, organizations can mitigate risks faster and with greater accuracy than ever before.

The sophisticated tool automatically extracts artifacts, analyzes data, and summarizes alerts and cases, offering detailed task lists with response recommendations. Sapphire AI enhances the Cerulean AI platform by harnessing the power of machine learning and automation.

Seamless Integration & Continuous Evolution

One of Sapphire AI's greatest strengths lies in its seamless integration with existing security tools and infrastructures. By centralizing visibility and simplifying workflows, it eliminates operational silos and ensures that security operations are cohesive and efficient. With its ability to reduce analyst time spent investigating benign cases by 70%, Sapphire AI empowers teams to focus on critical threats, enhancing overall operational effectiveness. Its cloud-native design ensures scalability, allowing organizations to expand their defenses as they grow without compromising performance.

Unlike legacy SOARs, Sapphire AI is not static. It evolves continuously through adaptive learning, incorporating real-time threat intelligence and lessons from past incidents to refine its capabilities. This continuous evolution enables it to combat both current and emerging threats, keeping organizations resilient in the face of an ever-changing threat landscape.

Sapphire AI's ability to combine adaptability, scalability, and cutting-edge technology makes it a future-ready solution that redefines what's possible in cybersecurity operations. By unifying diverse tools and workflows, it creates an integrated security ecosystem capable of tackling even the most sophisticated attacks.

Conclusion

The era of SOAR has come to an end. As cyber threats become increasingly complex and AI-driven, static platforms are no longer sufficient to meet the demands of modern security operations. Sapphire AI Insights exemplifies the next generation of cybersecurity solutions, combining adaptive intelligence, real-time responsiveness, and seamless integration to deliver unmatched protection. By transitioning to AI-powered solutions like Sapphire AI, organizations can enhance their ability to detect, mitigate, and recover from threats, ensuring a proactive and resilient security posture. The future of security operations lies in embracing innovation, and Sapphire AI is leading the way in this transformative shift.

AGILEBLUE

AgileBlue Cerulean AI combines AI-powered cybersecurity with the human touch you trust. Our SecOps platform autonomously detects, investigates, and responds to endpoints, network, and cloud cyber-attacks faster and more accurately than a legacy SOAR or SOC.

Our technology is both intelligent and automated, but we take a custom approach for every client we work with, analyzing and detecting exactly what matters most. Our products are entirely cloud-based with advanced machine learning and user behavior analytics, all supported by our U.S.-based team of cyber experts.

For more information, visit our website: AgileBlue.com.

Ready to start protecting your company?

Request a Demo of Sapphire AI