**Reduce Security Alert Fatigue by SOARing with AI**

* The average organization receives more than 11,000 security alerts per day.[[1]](#footnote-1)
* Up to 70% of alerts go uninvestigated.[[2]](#footnote-2)
* 78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio; 12% have 46 or more.[[3]](#footnote-3)
* It typically takes 13–18 minutes to classify a system-generated alert as a false positive or a possible attack.[[4]](#footnote-4)

The number of differing security products used by organizations today continues to grow, adding not only management complexity but also nuisance “alert swarms”—up to half of which are false positives.

Fortunately, MSPs and MSSPs typically have skilled security teams in place. Leveraging these skills to serve as many customers as possible—without compromising on service quality—makes each minute of each team member valuable. But having overtaxed security teams constantly switching between disparate products to address potential threats drives up time, effort, and risk.

Leveraging AI and machine learning and single pane of glass management, SOAR platforms can help organizations automate repeatable tasks that lead to alert fatigue and re-focus security analysts and engineers on investigating and remediating real threats. And it enables you to add strategic value to your customers’ businesses.

**What is SOAR?**

SOAR—security orchestration, automation, and response—solutions have become a popular enabling technology, allowing traditional MSPs and MSSPs to go beyond basic management and monitoring to rapidly transform into an MDR service provider business.

When it comes to security, it’s no longer enough to keep pace. Your customers demand a partner that can think beyond and help them stay ahead of the advanced attacks that can take out their business.

But managed services providers (MSPs) and managed security services providers (MSSPs) have traditionally focused on device management and monitoring, leaving a widening gap in their business models that’s increasingly being filled by managed detection and response (MDR) service providers. Fortunately, that’s changing.

* 50% of organizations will be using MDR services by 2025 for threat monitoring, detection and response functions that offer threat containment capabilities.[[5]](#footnote-5)
* By 2025, 33% of organizations that currently have internal security functions will attempt and fail to build an effective internal SOC due to resource constraints, such as lack of budget, expertise and staffing.[[6]](#footnote-6)

**5 Benefits of SOAR for MSPs/MSSPs**

1. **Comprehensively integrate security tools** – A SOAR platform enables you to integrate different types of security tools from various vendors, freeing up analysts for more strategic work instead of having them piece together the threat puzzle.
2. **Better utilize your security team** – Unlike a SIEM tool, SOAR platforms leverage AI to automate the processes needed to detect and resolve issues, minimizing human intervention and optimizing the time needed to detect, analyze, and remediate security incidents.
3. **Quickly detect and resolve threats** – Using AI, a SOAR platform provides “instant readiness” that enables your team to quickly evaluate known and unknown threats, scan for trends, assess historical data to detect patterns, and rapidly isolate suspicious activities or confirmed threats.
4. **Automate and orchestrate workflow processes** – Again, unlike a SIEM, a SOAR platform automates the process from investigation to remediation, significantly reducing the time needed to analyze alerts.
5. **Unify security tools** – SOAR quickly integrates security teams and tools to automate tasks, via AI and machine learning, that are then applied via playbooks. The result is a more proactive response and remediation of alerts and less time spent on manual intervention.

How can you grow your business with SOAR? Tune in for our next article on AI related trends and more. You can also contact the CyberSolv team now: [SecureNetworking@tdsynnex.com](mailto:SecureNetworking@tdsynnex.com).

1. “Managing Security Alerts with an Incident Response Platform,” SecurityBoulevard.com, 09/02/2022. [↑](#footnote-ref-1)
2. # “Managing Security Alerts with an Incident Response Platform,” SecurityBoulevard.com, 09/02/2022.

   [↑](#footnote-ref-2)
3. “The Top 8 Security and Risk Trends We’re Watching,” Gartner.com, 11/15/2021. [↑](#footnote-ref-3)
4. “Improve Threat Classification Accuracy with Supervised Machine Learning,” SecurityIntelligence.com, 01/06/2017. [↑](#footnote-ref-4)
5. “SOC Model Guide,” Gartner.com, 10/19/2021. [↑](#footnote-ref-5)
6. “SOC Model Guide,” Gartner.com, 10/19/2021. [↑](#footnote-ref-6)