Siemplify

THE BUSINESS CASE FOR SOAR

WHITE PAPER

Executive Summary

In the ongoing battle against cyber threats, it has never been more important for security operations teams to be sure they have the right tools in their arsenal. Security orchestration, automation and response (SOAR) platforms are rapidly becoming a must-have solution for SOC teams to enable more effective and efficient detection, triage, investigation and remediation of threats.

Yet, most security operations teams already face tool overload, and making the case to add yet another technology can be an uphill battle. However, unlike many detection and prevention tools, it is easy to calculate and quantify the potential ROI of a SOAR platform.

This paper details the various ways SOAR solutions can save security operations organizations millions of dollars annually through increased efficiency and better resource allocation. Enterprises generally see these savings spread across four key areas: alert handling costs, reporting costs, analyst training costs and miscellaneous operational costs. SOAR solutions also provide organizations with multiple benefits that are less quantifiable yet still provide value to the organization.

SOAR isn't just a mechanism for integrating security tools. Rather, it can transform the way security operations teams work, yielding real, tangible value to enterprises and managed security services providers (MSSP) alike.

ENTERPRISE SAVINGS WITH SOAR			
70%	60%	90%	80%
REDUCTION IN ALERT HANDLING COSTS	REDUCTION IN ANALYST TRAINING COSTS	REDUCTION IN REPORTING COSTS	REDUCTION IN PLAYBOOK CREATION COSTS

Why SOAR?

Enterprises and MSSPs face dozens of security operations challenges, though four major roadblocks seem to rise to the top of the list:

- **Alert overload and fatigue**
- **Inconsistent, undocumented and manual processes**
- **Piecemeal alert investigations involving tools that don't readily work together**
- **Ongoing skills shortage in information security**

While it may seem counterintuitive to add yet another technology to the mix, it makes sense for enterprises and MSSPs to consider investing in a security orchestration, automation and response (SOAR) solution to address the myriad challenges facing their security operations teams. SOAR solutions enable organizations to get more out of the security technologies in which they've already invested, codify and automate incident response processes and streamline day-to-day security operations activities. In this way, SOAR is unlike other information security expenditures in that it doesn't function as a 'lock on the door' or an 'alarm system'. Rather it helps SOC teams bring together their people, processes and technologies in a more intuitive, usable way.

Calculating Savings for Your Business

How do enterprises and MSSPs determine their potential SOAR ROI?

It's actually pretty easy. All it takes is knowing the number of alerts the SOC gets on a regular basis and understanding current operational and staffing costs. From there, calculating potential savings can be done across four key areas.

Alert Handling

Reporting

Analyst Training

Operational Activities

To provide tangible savings numbers, all examples in this paper are based on a SOC with the following attributes:

- 1,000 alerts per week
- 10 SOC analysts on staff
- $40 fully loaded hourly cost per security analyst
- 5 new hires each year (representing net new & turnover)

Additional assumptions related to specific savings are detailed in each section.

Alert Handling

All alerts are not created equal. Criticality varies as does the amount of attention and expertise required to effectively handle them. SOAR solutions increase analyst efficiency in handling three types of alerts: trivial, meaningful investigation and detailed investigation and remediation.

Trivial Alerts

Trivial alerts consist of false positives, redundant alerts and other notifications that don't pertain to meaningful events. It doesn't take long for analysts to dismiss each of these alarms once identified – maybe two to three minutes each. But because the vast majority of alerts fit into this category, they take up a significant percentage of analysts' valuable time and energy. In short, they're a time suck.

The value of a SOAR solution is huge in handling trivial alerts. Enterprises get the ability to easily close up to 70% of all the alerts that come into the SOC without any human interaction. This alone can equate to a savings of more than 90% annually.

Meaningful Investigation Alerts

Determining the criticality of this type of alert typically includes several manual steps across a number of consoles. And that's before an investigation can even begin. Meaningful investigation alerts are those that don't clearly fit into the trivial bucket and merit a deeper look plus some level of analysis. They require a level of critical thinking and take more of an analyst's time - from several minutes to several hours, and extreme cases, even days.

While these alerts generally aren't good candidates to be closed automatically, SOAR solutions can help streamline data gathering and enrichment to save precious time. Some SOAR solutions also provide context and visualization to enable more effective investigation. These typically result in an average efficiency gain of 80% for handling meaningful alerts.

HOW SOAR STREAMLINES ALERT HANDLING

Alert Clustering
By automatically grouping related alerts, SOC analysts are able to work threat-related cases, ultimately reducing their overall number of tasks and enabling the closure of multiple alerts in a single investigation.

Contextual Enrichment
SOAR solutions bring together details from across an organization's environment, enabling an analyst to cross-reference SIEM alerts with threat intel, EDR data, vulnerability info and more in a single view. The automatic fusing of this information gives analysts the deep context they need to holistically investigate threats.

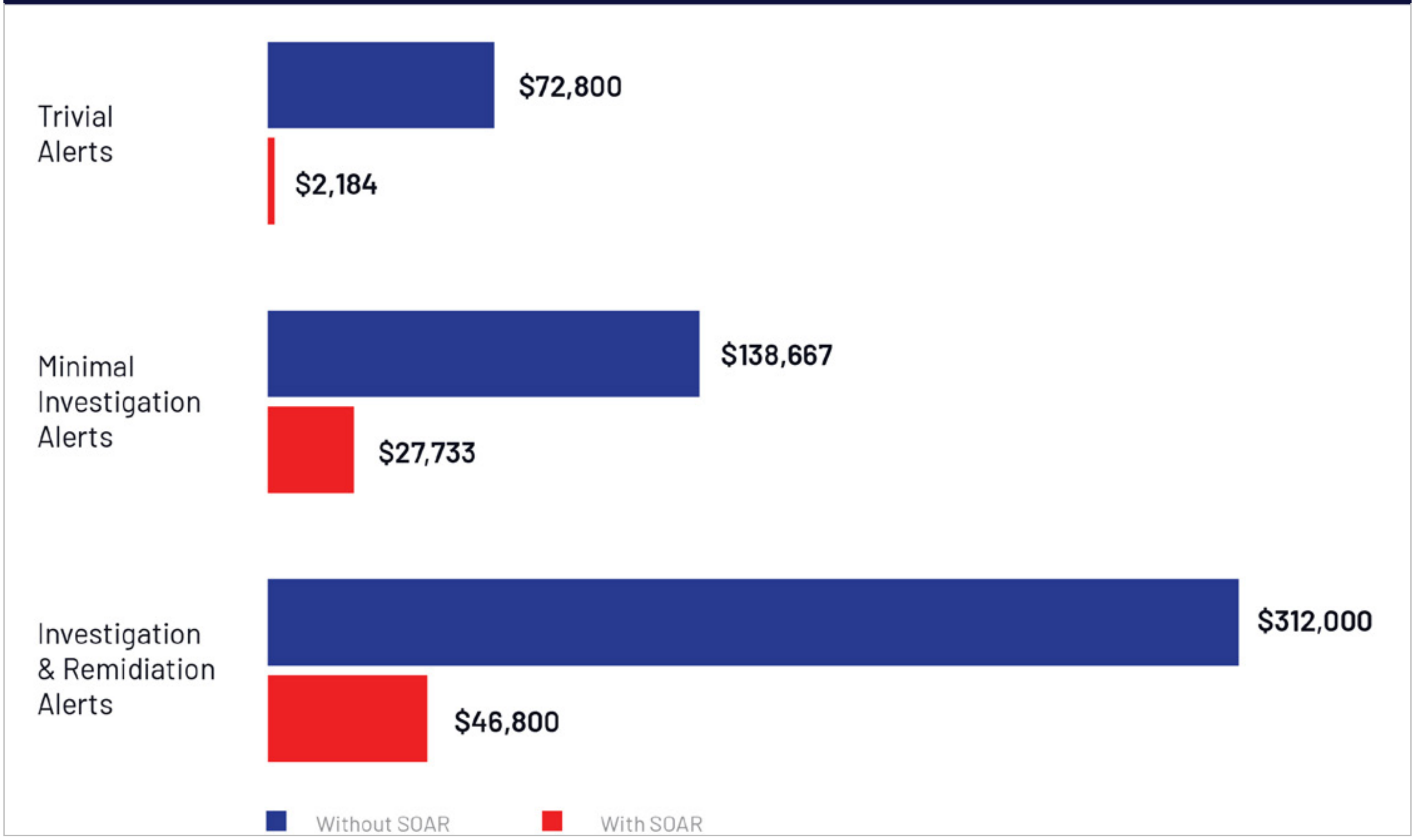
Playbooks & Automation
Inconsistent, manual processes slow down security operations teams. SOAR solutions help SOC teams create standardized, repeatable playbooks that can be automated to focus analyst activity on tasks that require critical thinking.

Detailed investigation and remediation alerts

The third category of alerts represents those that require the most analyst involvement and expertise – meaning, they take the most time. Detailed investigation and remediation alerts are those that likely represent truly malicious activity and require the most steps to address in order to return to a known good state.

In the previous sections, we noted that investigating alerts takes significant time and requires several manual steps, many of which can be automated through a SOAR solution. For these most critical alerts, enterprises can get additional efficiencies through automation of certain remediation efforts, such as blacklisting, changing user access or ordering the reimaging of a machine. Through the use of SOAR playbooks, organizations can reduce analyst time spent on these alerts from 90 minutes to just a few, resulting in savings of up to 85% annually.

ANNUAL ALERT HANDLING COSTS



Reporting

Whether to satisfy compliance auditors or internal stakeholders, security operations teams must be able to report on their activities and the outcome of their efforts. In most enterprise SOCs, this represents yet another arduous, manual effort, requiring analysts and managers to piece together data from across disparate consoles.

Through the use of a unifying platform like SOAR, security operations teams can make alert-specific and managerial reporting more turnkey and automated, saving significant time and effort.

Alert-specific reports

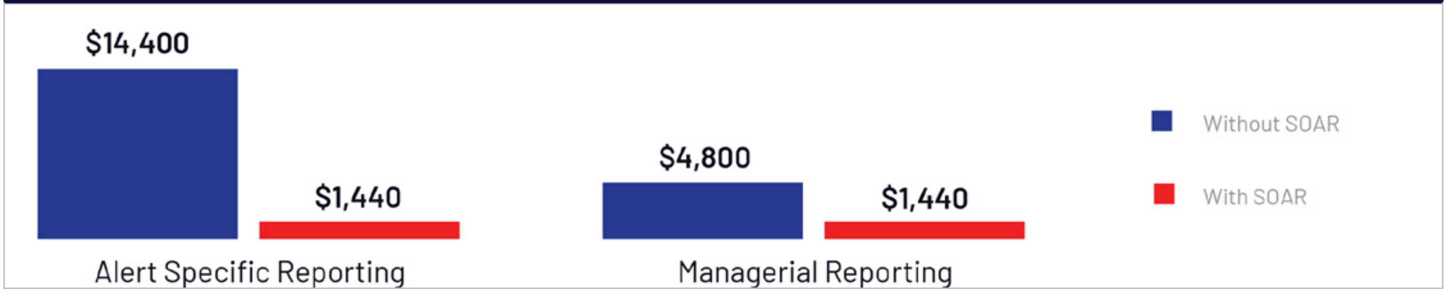
Usually required for audits, alert-specific reports provide a step-by-step description of what incident responders did to address a potential threat. Many SOCs spend upwards of 30 hours a month gathering data across consoles to manually generate these kinds of reports.

A SOAR solution reduces reporting efforts in two ways. First – simply by having most of the necessary data in a single pane of glass, analysts can look to a single console for all the detail they need. Second – many SOAR solutions include templates and automated reporting that give analysts the ability to generate required reports with a single click. Reducing time spent on reporting efforts gets analysts refocused on actually detecting and remediating threats while reducing reporting costs by up to 90%.

Managerial reporting

Managerial reports provide insight into security operations performance. They help answer questions related to how many alerts the SOC receives a week, how many alerts each analyst handles and how quickly as well as the overall mean time to detect (MTTD), mean time to respond (MTTR) and dwell time for the organization. Like alert-specific reports, these write-ups take significant time and effort to generate. Through KPI dashboards and automated stakeholder-specific templates, SOAR solutions can greatly reduce the time and costs associated with managerial reporting by an average of 70%

ANNUAL REPORTING COSTS



Analyst Training

Onboarding new analysts

Training new analysts can be a daunting task. New analysts need time to get acquainted with the SOC's technology stack and processes. In the absence of documentation, they ask senior analysts for guidance. These constant questions create distractions and consume time. And, it is likely that three senior analysts will give three different answers to the same question.

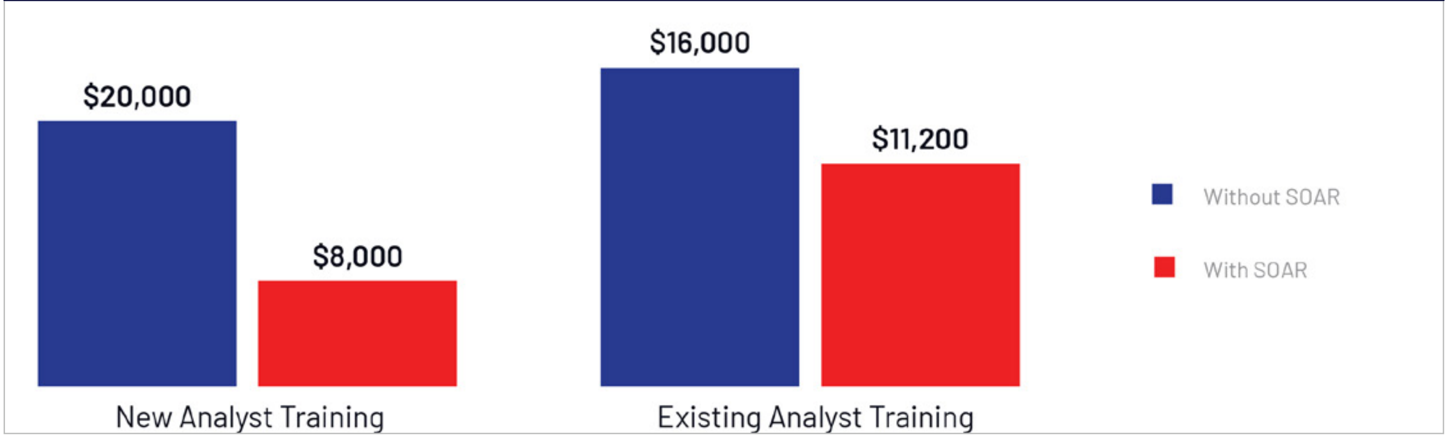
This reliance on "tribal knowledge" creates inconsistency within the SOC that contributes to longer ramp-up times for new analysts. Undocumented processes and disparate technologies typically mean a security operations organization will need to spend nearly 100 hours – the equivalent of 2.5 weeks – getting a single new analyst up to speed.

Continued Learning for Existing Analysts

Even your most experienced analysts never stop learning. New attack vectors and new technologies necessitate additional training for existing SOC analysts that can add up to about 40 hours per year.

SOAR solutions simplify analyst training on both technologies and processes. As a unifying fabric for a SOC's security stack, SOAR solutions reduce the number of tools and consoles an analyst needs to learn to do his or her job. And with built-in frameworks for standard playbooks and workflows, SOAR solutions help security operations teams create a repository for consistent, repeatable processes to be used by every single analyst in the SOC.

ANNUAL ANALYST TRAINING COSTS



Operational Activities

Inconsistency in day-to-day security operations reduces efficiency and increases overall operating costs. Because SOAR solutions help establish codified and consistent investigation, response and remediation processes, SOC teams can save meaningful time and money on daily operational activities.

Shift handover costs

Security operations is a function that never sleeps. Most enterprise and MSSP SOCs are 24x7 operations, which means analysts work in shifts and handoff investigations to one another each day. When processes and technologies are decentralized, the shift handover process gets more complex, more time consuming and is more fraught with risk that something may get missed. And having analyst shifts overlap to enable handoffs means doubling up on payroll costs.

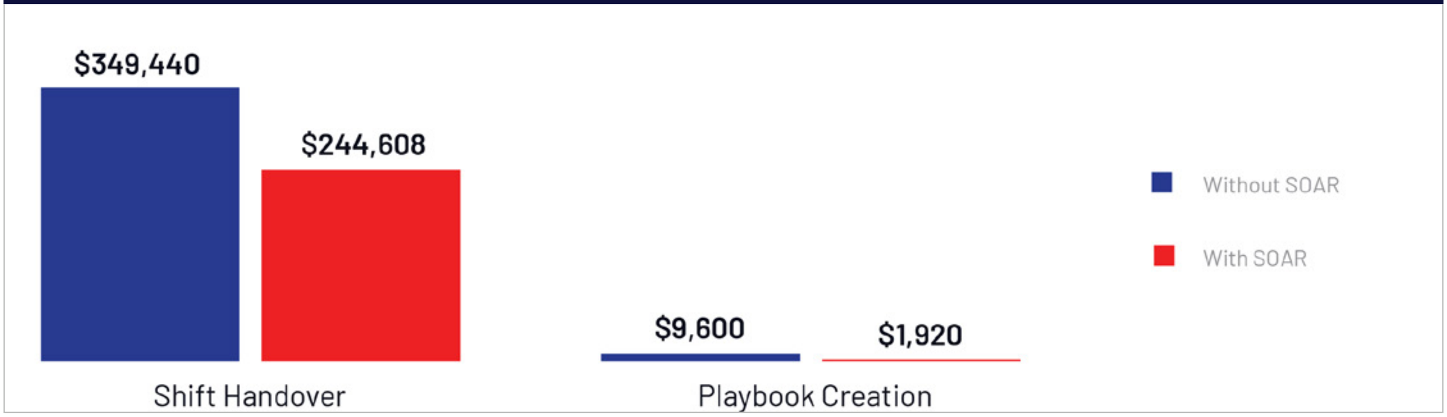
Many SOAR solutions come with shift management modules designed to reduce the overlap window, automatically assign cases to analysts and automate escalations. The right SOAR solution can yield a 30% savings on costs associated with shift handovers.

Playbook creation costs

Building, testing and maintaining playbooks is a vital function in any security operations organization. Physical playbooks can quickly become unwieldy and are time-consuming to maintain. And building workflows in Python may mean bringing on – and paying for – talent that doesn't currently exist within your SOC.

Using SOAR, security analysts can build automated playbooks using drag-and-drop functionality that even the newest analyst can effectively use. Most SOCs can expect savings of about 80% using this approach.

ANNUAL OPS ACTIVITY COSTS



Additional Benefits

In addition to the savings outlined above, SOAR provides organizations with other tangible benefits that aren't as easy to calculate in hard numbers but provide significant value, nonetheless.

Improved Analyst Morale & Reduced Turnover

Life for entry-level analysts can be pretty mundane. Most spend the majority of their days combing through rows of alerts in hopes of teasing out real threats from noise. According to Dark Reading, these mundane, repetitive tasks of the entry-level analyst make up just one of the reasons why there's such a high turnover rate in the SOC.

SOAR solutions enable the automation of the vast majority of Tier 1 analyst tasks, enabling these professionals to use their time for higher-level, higher-value tasks. Over time, these Tier 1 analysts begin to look like Tier 2 in their daily responsibilities, a transformation which adds value to the business and improves morale.

Retention of Internal Knowledge

When there are few documented processes in a security organization, tribal knowledge becomes the mechanism for getting things done. This works only for as long as the team remains intact. When someone leaves, their experience and knowledge walks out the door with them.

SOAR helps SOCs retain this tribal knowledge by capturing and documenting it into playbooks. Playbooks equalize resources and knowledge across the SOC and help maintain consistency in the face of new hires and staff turnover.

Reduced Dwell Time

The global median dwell time in 2017 was 101 days. That is a significant amount of time for a threat actor to be in your environment and can result in significant damage to your organization and its reputation.

The automation, visual investigation, context and playbook capabilities inherent in SOAR platforms speed up incident response efforts which ultimately leads to faster mean time to detect (MTTD), mean time to respond (MTTR) and lower dwell time metrics.

Reduced Organizational Risk

According to Cisco's 2018 Annual Cybersecurity Report, nearly half of security alerts go uninvestigated. This represents huge organizational risk and is a significant reason why dwell times are so high across the globe.

Through the alert grouping, case management and automation attributes of SOAR, analysts can handle more alerts faster, with less effort. This means there are fewer security issues which analysts fail to see, investigate and resolve.

What a SOAR investment looks like

When shopping for a SOAR solution, you'll run into two types of pricing structures: per automation step and per analyst.

Per automation pricing necessitates that you have a good idea of the number of activities you'll want to automate and can keep that number consistent. Most SOCs can't accurately estimate this over the long-term, which ultimately makes this structure highly unpredictable and tough to budget over multiple years. Some organizations find this pricing to be attractive at first but then feel restricted in their ability to use the solution to its fullest extent without it becoming cost-prohibitive.

Per analyst pricing means buying licenses based on the size of your SOC. Under this arrangement, security analysts can use the platform as much as they want, with no restrictions set for playbooks or automation steps. Generally, most security operations organizations have a good idea of how many security analysts they'll have over the next three to five years, which allows for longer-term budgeting and planning.

Calculating Total Savings With SOAR

Based on the various attributes we've explored, our example SOC can expect to save upwards of $5.7 million each year by using a SOAR solution to streamline its daily operations and increase efficiency.

SAVINGS WITH SOAR	
Alert handling savings	$446,749
Reporting savings	$16,320
Analyst training savings	$16,800
Operational savings	$112,512
TOTAL	**$592,381**

About Siemplify

Siemplify is a security orchestration, automation and response (SOAR) provider that is redefining security operations for enterprises and MSSPs worldwide. Its holistic security operations platform is a simple, centralized workbench that enables security teams to better investigate, analyze, and remediate threats. And, using automtated, repeatable processes and enhanced measurement of KPIs, Siemplify empowers SOC teams to create a culture of continuous improvement. Siemplify's patented context-driven approach reduces caseload and complexity for security analysts, resulting in greater efficiency and faster response times. Founded by Israeli Defense Forces security operations experts with extensive experience running and training numerous SOCs worldwide, Siemplify is headquartered in New York with offices in Tel Aviv.

Siemplify

siemplify.co