WHITE PAPER

Measuring the ROI of Security Orchestration and Response Solutions

splunk>

turn data into doing™

Investing in a security orchestration and response (SOAR) solution is a wise and highly strategic decision. Choosing the right solution to build your security operation center (SOC) on is arguably more important than choosing any security point product. The SOAR solution you choose will become a central part of your security infrastructure, effectively acting as the operating system for your security investments.

SOAR solutions produce a number of economic benefits in addition to helping your SOC team work more efficiently. This white paper aims to quantify those benefits by outlining a methodology to estimate your return on investment (ROI) from investing in a SOAR solution.

Why Are SOAR Solutions Needed?

Your security team is hard at work on the front lines: identifying, analyzing and mitigating the threats facing your organization. Despite its best efforts, however, the team's alert and case backlog likely grows larger every day. The reality is that there simply aren't enough skilled professionals to analyze the volume of alerts that most organizations face daily.

The attackers are industrialized. Threats continue to grow more sophisticated, increase in volume and will likely evolve into a new attack before you've had the opportunity to address the previous one. The dwell time for threats in your environment — the time needed to detect and remediate attacks — is growing despite increases in security spending.

Compounding security teams' challenges is the reality that the complexity of our IT environments continues to increase. This is true for security as well; we've now been deploying point security products for over three decades. In fact, research shows that there are more than 1,500 vendors selling security products and services today. Another grim fact is that most security products lack interoperability, leading to a horde of independent solutions that require a room full of people just to maintain them. Despite bundled offerings from some of the largest security vendors, many organizations still prefer to buy best of breed — and for good reason. The end result is a heterogeneous collection of individual security products with no interconnectivity or ability to function as a single unified defense solution.

You know something has to change. You've already made a large security investment in both talent and technology. You want to better leverage your existing resources by deploying tools that maximize efficiency and scale to create a unified defense system that is greater than the sum of its parts.

SOAR solutions have become the force multiplier needed to unlock the full power of an organization's security investment toward solving these problems. Designed from the ground up for security-specific automation and orchestration, leading SOAR solutions unify point products using a logical architecture that abstracts product capabilities into security actions that can be easily automated using digital playbooks.

What Are the Benefits of SOAR?

SOAR solutions help you work smarter by automating repetitive tasks, multiplying your team's efforts and allowing it to focus its attention on the mission-critical decisions that require its talents. SOAR solutions can:

- Automatically triage events to eliminate noise from your workload
- Pre-fetch threat intelligence to support your decision making
- Orchestrate complex workflows to improve efficiency and precision

89% of respondents noted that on average, their security operations center (SOC) saved up to 5 hours of work per day per analyst after deploying SOAR.
– **EMA Research, 2020**

SOAR solutions also help you respond faster and reduce dwell times with automated detection, investigation and response. They help you:

- Execute actions in seconds instead of minutes, hours or more if performed manually
- Create complex workflows using security-specific actions that apply to multiple security products
- Build playbooks quickly and without coding using a visual playbook editor

Finally, SOAR solutions help you strengthen your defenses by integrating your entire security infrastructure together so that each part is actively participating in your defense strategy.

- Deploy vendor-supplied or custom app integrations to unite all of the security tech you're using
- Leverage the security data provided by one technology to guide and inform downstream actions using another technology
- Improve security by reducing your mean-time-to-resolution (MTTR)

Prior to SOAR deployment, security teams indicated that their MTTR was around one to four hours for a given incident. After SOAR deployment, they saw their MTTR decreased to 30 to 60 minutes.
– **EMA Research, 2020**

Beyond the economic return, deploying a SOAR solution also improves consistency as the same data is gathered for every event and every event is investigated the same way, every time.

The ROI for One Splunk SOAR Customer

Many customers begin with incident response (IR) use cases when deploying SOAR solutions. Automating the investigation of suspected phishing emails is a common scenario — the investigations are highly repetitive, follow a known process and consume valuable analyst time when performed manually.

One Splunk® SOAR customer used the solution to automate a process that took more than 90 minutes to complete manually. A typical day for this customer might bring as many as 45 phishing emails for the security team to investigate. The standard operating procedure for this type of event includes acknowledging receipt from the employee, analyzing the email for malicious indicators and taking steps to remediate if the email is confirmed as part of a phishing campaign. From start to finish, the process might take more than 90 minutes for each suspected phishing email.

Using actual data from this customer's deployment and estimated salary data for a Tier-1 SOC analyst, we can compute the cost of handling the phishing investigations and response manually:

Table 1	Before Splunk SOAR (on an average day)	After Splunk SOAR (on an average day)	Expected savings with Splunk SOAR
Number of Phishing Emails/Day Resolved	45	45	
Average Hour Salary for a Tier-1 Analyst[1]	$37.11	$37.11	
Estimated Time Required to Manually Handle Each Phishing Email	90 minutes	40 seconds	89 minutes saved per day on a containing a given phishing email
Daily Cost to Handle Phishing Emails	$2,504	$18	$2,486 savings per day
Annual Cost to Handle Phishing Emails[2]	$515,824	$3,708	$512,116 savings per year

[1] Source: https://www.glassdoor.com/Salaries/security-analyst-salary-SRCH_KO0,16.htm
[2] Five-day work week assumed.

With automation, the entire process now completes in under a minute, freeing the team to focus time on less routine investigations that require a human's insight. This 98% reduction in the time required to handle a phishing email equates to savings of over **$512,116 savings per year**.

While the savings possible from handling just the phishing emails on a routine day alone can justify the acquisition of a SOAR solution, the expected return on investment is even greater.

Routine days for the team mean 45 phishing emails to address, which is a heavy workload for a SOC team. This Splunk SOAR customer also occasionally observes burst attacks with up to 300 phishing emails in a single day. Using the data presented above, we can also estimate the return associated with handling burst attacks.

Table 2	Before Splunk SOAR (burst attack)	After Splunk SOAR (burst attack)	Expected savings with Splunk SOAR
Number of Phishing Emails/Day Resolved	300	300	
Average Hour Salary for a Tier-1 Analyst[1]	$37.11	$37.11	
Estimated Time Required to Manually Handle Each Phishing Email	90 minutes	40 seconds	89 minutes saved per day on a containing a given phishing email
Daily Cost to Handle Phishing Emails	$16,700	$123	$16,577
Annual Cost to Handle Phishing Emails[2]	$400,800	$2,952	$397,848

1. Source: https://www.glassdoor.com/Salaries/security-analyst-salary-SRCH_KO0,16.htm
2. Two burst attacks per month assumed.

If the customer is saving **$512,116 savings per year** for normal levels of phishing attacks daily and **$397,848 savings per year** for two burst attacks per month, that will equate to saving **$909,964 per year** on just resolving phishing email attacks.

Savings per year for handling 45 phishing emails a day[1]	$512,116
Savings per year for handling 300 additional phishing emails twice a month[2]	$397,848
Total savings per year	$909,964

1. From Table 1.
2. From Table 2.

With the same 98% reduction in the time required to handle a phishing email, the total savings equates to about $1 million per year. Since additional analysts cannot be staffed "on demand" to handle burst attacks and the full-time team lacks the capacity to address them, most of the phishing emails received during a burst attack are simply ignored. The true cost of the phishing problem could be much higher after considering the potential breach costs stemming from an incident that has gone unchecked.

> **Automation with Splunk SOAR enables us to process malware email alerts in about 40 seconds vs. 30 minutes or more.**
> – CISO, Blackstone

What Other Use Cases Are Important?

Though IR is a common use case for SOAR solutions, industry leading solutions, like Splunk SOAR, are open and extensible for other use cases. This flexibility gives SOC teams the ability to easily automate a wide range of standard operating procedures (SOPs).

Teams often focus initially on use cases that represent their greatest pain points. These use cases often contain many manual tasks and require working across multiple products and departments to complete a single playbook.

While the acquisition of a SOAR solution can often be justified by a single use case, it's still important to consider other potential use cases. This effort should involve key stakeholders across your security operations team. Developing comprehensive security use cases is important to help ensure that the solution you choose today will also support your needs in the future and maximize your ROI.

The following use cases are also popular and span the investigation, enrichment, containment and remediation categories:

Alert Triage

The objective with alert triage is to validate and prioritize incoming alerts. Use cases that focus on triaging inbound alerts involve enriching events with additional context. They may also include logic to eliminate high-confidence false positive alerts from further processing.

Indicator of Compromise (IOC) Hunting

By automating IOC hunting, teams can fully leverage the threat intelligence they receive instead of limiting the IOCs they hunt for due to resource constraints. They might also implement intelligence scoring to assist with deciding which threat intelligence sources to use.

Vulnerability Management

Automating the cycle of identifying, classifying, remediating and mitigating vulnerabilities yields not only greater team efficiency, but also more consistent results by ensuring that the process is performed the same way every time.

Network Access Control (NAC)

SOAR solutions can augment dynamic access control strategies. One example is integrating a detection system that previously was not part of the NAC decision-making logic.

User Management

Ensuring that users are enabled and disabled accurately, rapidly and systematically can eliminate the chance that a user account is used maliciously by a threat actor.

Penetration Testing

Activities like asset discovery, classification and target prioritization can be automated, thus increasing the productivity of the pen testing team.

Intelligence Sharing

Organizations that have intelligence sharing initiatives can greatly benefit from an automation-assisted playbook. Automation can also increase an analyst's productivity and provide time-sensitive information back to a community faster than with manual processes.

Any well documented SOP in which the security operation team can easily codify the criteria for automation is a good candidate for SOAR solutions. Ultimately, a larger collection of automated playbooks leads to even better ROI as the cost of the solution is amortized over more use cases.

Conclusion

SOAR solutions produce strong economic returns while helping organizations work smarter. By automating repetitive tasks, teams can respond faster and reduce dwell times with automated detection, investigation and response. They can also strengthen their defenses by integrating the entire security infrastructure together so that each part is actively participating in the defense strategy.

Whether you intend to start with a common use case from the incident response category or one from a different category, it's important to consider your ROI as part of the decision. While this paper provides an overview for common use cases and an approach to estimate ROI for SOAR solutions, other resources are available.

To learn more about the Splunk security automation and orchestration solution, download the free Splunk SOAR Community Edition or ask sales for more information.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com