WHITE PAPER

SOAR 101: An A-to-Z Guide That Answers All Your Questions About SOAR.

Learn All About the Fundamentals of SOAR, How SOAR Elevates Your SecOps, and How to Make the Best ROI Out of Your SOAR Investment.

DFLABS.COM

Automate.
Orchestrate.
Measure.

DFLABS
CYBER INCIDENTS UNDER CONTROL

Contents.

Introduction 1

SOAR Definition: What is SOAR? 1

What is a SOAR platform? How is it Different From SIEM? 2

Does SOAR Replace SIEM? 2

Why is SOAR Becoming Increasingly Prevalent in the Cyber Security Industry? 3

How Does SOAR Affect the Incident Response Efficiency of One SOC? 4

How Does Progressive Security Automation Function? Is Automation Dangerous? 4

The Role of SOAR in Cyber Security 5

How Does SOAR Fit Into a Security Network? 6

Why is Improved Incident Response Time Such a Valuable Aspect of What SOAR Offers? 6

Is SOAR a Replacement for Other Security Technologies? 7

What Kind of ROI Should I Expect by Investing in a SOAR Solution? 8

Do all SOAR Vendors Offer a SOAR Solution With the Same Quality? 8

How to Distinguish the Best SOAR Solution for Your Needs? 9

Investing in a Strong SOC Team Without SOAR Will Downgrade Your ROI 9

Why Investing in a SOAR Solution Pays Off? 10

Evaluate the Needs of Your Organization 11

Learn how to Utilize SOAR's Strengths 11

Choose the Right SOAR Solution: What Makes IncMan SOAR the Best 12

Is SOAR Just for Structured Firms or is it Also for SMEs? 13

Conclusion 13

Automate.
Orchestrate.
Measure.

Introduction.

As a relatively novel technology in the cyber security industry, SOAR (short for Security Orchestration, Automation, and Response) is still settling in and yet to reach its full potential. But many still don't quite understand the value of SOAR in its entirety.

In this white paper, we will address the fundamentals of SOAR, dive deeper into the idiosyncrasies of security automation, and give a more thorough explanation of how SOAR fits in a typical SOC environment, how SOAR elevates your SecOps, and how to make the most out of your SOAR investment.

In short, we will delve into the very core of SOAR, unravel the essence of security automation and AI-enhanced SecOps, and explain just why this particular technology plays a major role in the heart of every cyber security team. Let's dive right in.

SOAR Definition: What is SOAR?

SOAR allows SOC teams to respond faster to cyber threats, recognize false positives by detecting patterns, and free time for analysts to be able to focus on more relevant threats that require in-depth expertise.

The SOAR acronym stands for Security Orchestration, Automation and Response. And the short version that briefly describes what is SOAR goes something like this:

- SOAR is a technology that allows companies to collect data regarding threats and alerts and allows analysts to respond to threats in less time and automate repetitive tasks.

Of course, now we're just scratching the surface. There is a whole lot more to SOAR than it meets the eye, and we'll take things one step at a time. Now, for the more elaborate definition that clears the fog and shines a light on the idiosyncrasies of SOAR:

- SOAR is a term coined by Gartner, which is used to describe three distinctive software capabilities. Orchestration, as a term, covers threat and vulnerability management, which include all the technologies that assist with the resolution of cyber threats.
- Automation refers to security automation, which describes the process of utilizing progressive automation and machine learning to automate particular areas of security operations.
- The term response refers to security incident response, which measures in detail how the organization responds to threats, in order to use that information to strategically increase the effectiveness of SecOps.

These three elements combined together make up the complex technology known as SOAR. Of course, understanding the SOAR definition and how SOAR operates is not that easy.

Still, as complex as it is, SOAR is still fairly straightforward to use, as the technology was created with the intention of instantly helping, not confusing security professionals. With the implementation of SOAR, the natural workflow of SecOps remains unaltered, yet it is drastically improved. SOAR allows SOC teams to respond faster to cyber threats, recognize false positives by detecting patterns, and free time for analysts to be able to focus on more relevant threats that require in-depth expertise.

But how can SOAR affect the way a SOC team operates without altering the core of their SecOps? This is possible because SOAR blends in the environment it is deployed in. SOAR is created with flexibility and swift customization in mind.

SOAR can integrate with a wide range of security tools, and instead of requiring security professionals to adapt to the way the technology operates, SOAR's amazing customization capabilities actually allow security professionals to preserve their conventional workflow and reap the benefits of SOAR at the same time.

What is a SOAR Platform? How is it Different From SIEM?

This is one of the most commonly asked questions about SOAR, as many still confuse its capabilities with another cyber security technology, known as SIEM. SOAR starts where SIEM stops. A SOAR platform is characterized as the environment where SOAR is deployed and the changes it inflicts on the particular security ecosystem:

- A SOAR platform is typically incorporated in a SOC in order to increase the efficacy of the security professionals working within the SOC. SOAR uses automation and orchestration to help organizations pinpoint real cyber threats, eliminate false positives, and respond to actual danger by drastically improving the incident response time.
- SIEM, on the other hand, is a modern data aggregator that is solely used to collect information regarding alerts. Unlike SOAR, which leans on a machine learning engine to be constantly up to date with the most contemporary cyber threats, SIEM requires frequent manual tweaking from a cyber analyst in order to maintain its contemporary status.

In other words, not only does SOAR collect data, but it uses its machine learning engine to single-handedly respond to threats and utilize automation to fully carry out low-risk tasks (like documenting the process of analyzing an alert) without the need of human interaction. SIEM differs from SOAR in the sense that SIEM delivers the data regarding a threat, without facilitating recommended courses of action, ultimately requiring security professionals to do the job of assessing every single alert manually.

Within a given platform, SOAR allows SOC teams to detect, assess, and remediate cyber incidents all-the-while decreasing the need for human intervention in the process by providing automated analysis and utilizing machine learning and AI. Whereas SIEM needs constant tweaks and updates in order to be able to differentiate between normal and suspicious alerts.

Within a given platform, SOAR allows SOC teams to detect, assess, and remediate cyber incidents all-the-while decreasing the need for human intervention in the process by providing automated analysis and utilizing machine learning and AI. Whereas SIEM needs constant tweaks and updates in order to be able to differentiate between normal and suspicious alerts.

This is why, with SOAR, analysts have more time to focus on higher priority assignments, rather than having to manually check every alert as it arrives in real-time, which is the case with those SOCs that rely on SIEM.

Does SOAR Replace SIEM?

This is a crucial thing to understand - no, SOAR does not replace SIEM. The reality is that SOAR and SIEM are two very different technologies, and while SOAR is superior to SIEM in some areas, there is a reason why so many companies use SIEM, after all.

SIEM stands for Security Information and Event Management. In short, SIEM's expertise lay in collecting and aggregating security information, including:

- **Data from firewalls**
- **Intrusion detection systems**
- **Network appliances**

However, once SIEM stores the aggregated data, its job is done. And in order to be able to replicate SOAR's behavior and differentiate between normal and suspicious alerts, SIEM requires constant tweaking, which is performed by security analysts and engineers. But while SOAR has

In order to be able to replicate SOAR’s behavior and differentiate between normal and suspicious alerts, SIEM requires constant tweaking, which is performed by security analysts and engineers.

the upper hand in this area, and can autonomously distinguish between normal and potentially malicious alerts, SIEM is better at generating large volumes of data regarding security alerts.

So, rather than having to choose between SIEM and SOAR, the wise thing to do would be to combine the strengths of these two very different technologies and leverage their benefits by unifying them in a singular SOC platform. By working together, SOAR will be able to react to every alert generated by SIEM in a timely and effective manner.

Why is SOAR Becoming Increasingly Prevalent in the Cyber Security Industry?

So far, we mentioned that SOAR utilizes orchestration and incorporates automation in SecOps. Now, we're going to explain just how these features benefit organizations, SOCs, MSSPs, and CISOs as well:

- **Resolve the alert fatigue problem:** Many organizations receive thousands of alerts on a daily basis, and SOCs often don't have the manpower to properly assess every one of them. The huge volume of alerts inevitably leads to an overload of work for analysts, who are unable to keep up with the never-ending flood of alerts. By leveraging security automation, SOAR replaces analysts by taking care of low-risk alerts, repetitive tasks, and false positives, which make up for over 60% of all alerts.
- **Addressing the skill shortage issue:** The number of daily alerts is rising, and sadly, the number of skilled security professionals is decreasing. However, SOAR directly addresses this issue by increasing the SOC productivity by 10 times, allowing SOC teams to accomplish more by doing less.
- **Drastically increasing incident response time:** SOC teams that don't rely on the most contemporary technology and are not stacked with the most skilled analysts are often too slow in analyzing alerts. SOAR allows security professionals to increase their response time to cyber threats by up to 80% with fully or semi-automated responses.
- **Elevate the efficiency of SOPs:** SOAR automates certain standard operating procedures (SOPs), such as generating reports and documentations. This relieves analysts from the duty of having to manually perform these tasks and allows them to focus their expertise on more important assignments.

The reason why SOAR is growing both in popularity and demand is that SOAR addresses the issues that couldn't be resolved by older technologies.

SOAR acts as an all-in-one solution, simultaneously reinforcing different aspects of one SOC. And Gartner believes that, in comparison to today's 5%, in 2022, over 30% of all SOC with over 5 members will rely on SOAR as their primary technology solution that connects all aspects of their security platform. Making it clear that the path of SOAR is already paved, and we're the ones who have to follow.

In comparison to today’s 5%, in 2022, over 30% of all SOC with over 5 members will rely on SOAR as their primary technology solution that connects all aspects of their security platform.

How Does SOAR Affect the Incident Response Efficiency of One SOC?

We already mentioned that SOAR improves the incident response time of an average SOC team by 80%. Yes, you read that correctly… 80%. But how exactly is that possible? Let us elaborate:

- Respond to threats within minutes instead of hours: SOAR uses its automation capability to get to the bottom of incoming alerts. Major companies get bombarded with thousands of threats every day, and without SOAR, answering every one of those alerts can take hours, days, and sometimes even weeks.
- In this scenario, SOAR presents a quick visual representation with every relevant characteristics of an alert, and given that SOAR is able to tell apart normal from suspicious alerts, SOAR will only notify analysts in case there is an unprecedented, complex issue that SOAR cannot resolve with the knowledge it already has. And, as we said that over 60% of all alerts end up being either false positives or low-risk threats, SOAR allows analysts to respond to the threats that really matter within minutes.

Instead of sifting through endless data, SOAR automatically presents the most relevant pieces of information regarding a threat, allowing analysts to make well-informed decisions from the powerful insights SOAR provides through its customizable dashboards.

And the beauty of it is that SOAR will remember the course of action taken to remediate complex threats, and thus increase its knowledge and be more competent to at least provide recommended courses of action when a similar threat appears in the future. This is what progressive automation is all about, and that's what we're going to explain in more detail in the heading below.

Even though many are skeptical about automation, the truth is, there is no reason to be scared of it, because even though SOAR has a machine learning engine backed by AI, it is still very much in control by analysts and engineers. In reality, SOAR's automation will operate in the way orchestrated by analysts, not the other way around.

How Does Progressive Security Automation Function? Is Automation Dangerous?

Security automation is often a subject of some of the most heated debates among security professionals. To automate or not to automate? But before answering that, let's delve into the idiosyncrasies of security automation:

- **Detect and resolve false positives:** Due to its machine learning engine, SOAR is capable of differentiating false positives from actual threats. The reason why security automation is called progressive is that the engine itself is programmed to accumulate knowledge from the characteristics of different types of threats it encounters, and SOAR uses that knowledge whenever an alert with a familiar pattern occurs.
- **Adjustable degree of automation:** Analysts can decide whether they want to fully or semi-automate certain processes. By configuring the documented procedures of a playbook, analysts have full autonomy to choose under which circumstances they want SOAR to fully automate certain tasks, and in which areas they want to include human intervention.

- **Security automation frees up analyst time:** SOAR's security automation revolves around utilizing artificial intelligence and machine learning to apply full or semi-automation to workflow processes. Given that many of the day-to-day processes of many SOCs are repetitive, automating those repetitive processes spares a lot of time that would be unnecessarily spent if those processes were handled manually by analysts.
- **Helps deal with the increasing volumes of alerts:** Given that analysts have more time on their hands thanks to security automation, they can redirect their valuable time to focus on mitigating malicious threats. And documenting playbooks, SOC teams actually allow automation to resolve the flood of low-risk alerts in a regulated manner, all-the-while complying with GDPR and NIST regulations.

Even though many are skeptical about automation, the truth is, there is no reason to be scared of it, because even though SOAR has a machine learning engine backed by AI, it is still very much in control by analysts and engineers. In reality, SOAR's automation will operate in the way orchestrated by analysts, not the other way around.

Even if you choose automation to take part only in low-risk processes, that would still be extremely helpful for your SOC team, as it will alleviate the burden of having to spend their time handling menial and repetitive tasks unnecessarily.

SOAR can be defined as the technology that allows companies to collect threat-related data from various sources and automate low-risk security processes.

The Role of SOAR in Cyber Security.

When we talk about SOAR, we often use the word solution. We refer to SOAR as a solution, which is suitable but can be somewhat confusing to the uninitiated. As we explained in the previous SOAR guide, SOAR can be defined as the technology that allows companies to collect threat-related data from various sources and automate low-risk security processes.

Of course, this definition doesn't do justice to the myriad of invaluable capabilities SOAR provides to SOC teams, so in order to understand the value of SOAR, let's unravel the role of SOAR in a typical SOC environment:

- **Force multiplier:** What most SOAR-newbies fail to realize is that the sole act of incorporating SOAR in a security environment won't do much. SOAR feeds on the abilities of other technologies and is created with the sole purpose of increasing the efficacy of a SOC environment. This means that SOAR doesn't replace other technologies, yet, it acts as a force multiplier and allows them to exceed their capabilities.
- **Connective tissue:** SOAR interacts with other technologies, such as SIEM, and builds on the knowledge extracted from such technologies to allow security professionals to make better incident-related decisions. SOAR also allows everyone on the SOC team to have a better understanding of the security strategy by offering a customizable dashboard that can be used to improve the communication among SOC members and also follow a wide range of valuable KPIs.
- **False positive detector:** Thanks to its machine learning engine, SOAR has the ability to successfully differentiate normal from suspicious activity and tell apart real threats from false positives. This is a capability that no other technology provides, and this feature is incredibly valued by analysts, in particular, as it frees their time from having to manually check every alert. Even the ones that are low-risk and probably don't pose a threat to the organization.

Thanks to its automation capabilities, SOAR allows clients to create documented playbooks which will allow them to fully or semi-automate repetitive and menial tasks. And, given that companies receive thousands of alerts on a daily basis, most of which fall into the category of low-risk alerts, this makes the presence of SOAR's automation an invaluable asset to every SOC team.

However, even though SOAR can replace human presence in low-risk assignments, it is still recommended to utilize SOAR's powers in a manner that will reinforce your SOC's incident response capabilities. SOAR will boost your incident response time by **up to 80%**, and in the meantime, it will **boost the productivity of your analyst by ten times** just by freeing their time with the act of automating thousands of menial and mundane tasks. In other words, it will allow them to have more time to focus on the threats that really matter.

Given that companies receive thousands of alerts on a daily basis, most of which fall into the category of low-risk alerts, this makes the presence of SOAR’s automation an invaluable asset to every SOC team.

How Does SOAR Fit Into a Security Network?

SOAR is extremely customizable, and instead of disrupting the natural workflow of security operations, SOAR blends into the environment it is deployed and allows security professionals to maintain their natural workflow of security operations. Regardless of the size of the organization, SOAR fits into every environment seamlessly and integrates well with both internal and external applications and technologies. SOAR is very easy to integrate with, as the technology allows clients to create bidirectional integrations with hundreds of security technologies.

Our own SOAR solution, IncMan SOAR, is particularly easy to integrate with, as the technology allows clients to create bidirectional integrations with hundreds of security technologies. IncMan SOAR adopts an Open Integration Framework philosophy, which allows clients to create their own integrations without our supervision and with little coding experience required. This all means that SOAR is meant to instantly accommodate to the environment it is deployed and make an immediate impact without causing any disruptions to the organization.

Why is Improved Incident Response Time Such a Valuable Aspect of What SOAR Offers?

One of SOAR's most respected capabilities is the ability to drastically improve a SOC's response time to incidents. That is simply because the more time it takes for you to assess a certain incident, the more time you allow hackers and other malicious actors to cause damage to your organization. And the bigger the breach time, the more serious the damage is.

This means that with every additional second of breach time, more damage is potentially inflicted on your organization. Sadly, many SOC teams are overwhelmed with large volumes of alerts, which they can't plausibly assess in record time. Sometimes, it can even take them hours, days, or even weeks to properly analyze an alert. And by that time, if the alert has proven to be an actual threat, the malicious actor will have already inflicted the intended damage. Whether it is to extract data, affect the organization financially, or impose damage in other ways, if the response time to such incidents is abysmal, the damage caused will be horrendous.

This is why, for those who have already witnessed the incredible power of SOAR, its ability to enhance incident response time is unexpendable. But how can SOAR improve response time to cyber threats by as much as 80%, you may ask? Well, some SOAR solutions, like our IncMan SOAR, run on a machine learning engine, which allows SOAR to read the characteristics of a certain threat, and depending on whether the analysts labeled that alert as a false positive or an actual threat, SOAR will remember the course of action taken and thus become capable of making accurate decisions when it encounters a similar threat in the future. In other words, SOAR detects the patterns of security alerts and predicts a successful response thanks to its AI-backed machine learning engine.

Also, SOAR automates over 60% of all security operations related to low-risk and repetitive assignments, which frees up plenty of time for analysts to be able to accurately intercept real threats and assess time in a timely manner. It's much easier to recognize the real threats when SOAR takes care of the thousands of alerts that are only meant to confuse analysts and waste their time while the real threats go by undetected.

One of SOAR's most respected capabilities is the ability to drastically improve a SOC's response time to incidents. That is simply because the more time it takes for you to assess a certain incident, the more time you allow hackers and other malicious actors to cause damage to your organization. And the bigger the breach time, the more serious the damage is.

Is SOAR a Replacement for Other Security Technologies?

What many security professionals fail to realize is that SOAR does not replace the necessity of having other security tools incorporated into your SOC. As we explained earlier, SOAR is a force multiplier, which means that the technology itself is not able to act as an incident responder and replace every other tool within the SOC. What it can do is that it can boost the productivity of virtually anyone on the SOC team, allow security professionals to make well-informed decisions thanks to its automation capabilities, and vastly improve the incident response time.

People shouldn't mistake SOAR for some magical tool that replaces every other technology in the cyber security industry. Yet, SOAR should be understood as the binding force that connects the dots in a SOC environment and improves the potential of every tool it interacts with.

In order to get the best out of SOAR, you should consider merging SOAR with other security tools. Combining the strengths of technologies like SOAR and SIEM will allow your SOC to flourish and drastically improve the quality of the SecOps. In other words, SOAR connects people, technologies, and processes with the goal of optimizing the efficacy of the entire SOC. But as advanced as SOAR may be, it is still a piece of software that must be led by the expertise of top security professionals and must be backed with the right tools and technologies necessary to combat evolved cyber threats.

What Kind of ROI Should I Expect by Investing in a SOAR Solution?

The ROI of SOAR differs from each respective organization and the way SOAR is being utilized. But, assuming that SOAR's capabilities are optimally utilized, the ROI from incorporating SOAR boils down to the following most important elements:

- **Improved time management and productivity:** By automating a myriad of repetitive tasks, analysts will have more free time on their hands to prioritize tasks and improve their efficiency.
- **Enhanced threat hunting capabilities:** SOAR's machine learning engine improves the SOC's threat-detecting abilities and provides analysts with thorough analysis regarding a threat which allows them to make a well-informed decision.
- **Increased efficiency:** Thanks to automation, you'll get more things done with fewer resources. SOCs will better allocate their resources, and analysts will be able to focus on tasks that really matter.
- **Improved employee retention:** Security professionals will have more pleasure in performing their activities, given that they don't have to manually handle menial tasks.

Bottom line is, the ROI of SOAR is going to be reflected by the way you utilize SOAR. And granted that you do make the most out of SOAR, you'll get more done in a shorter amount of time and with fewer resources. Companies that receive thousands of alerts every day will definitely make their money's worth by utilizing SOAR's progressive automation capabilities.

With that being said, in order to make the best ROI out of your SOAR solution, you must strategically assess the nature of your security operations. Either way, it's beyond any doubt that there is a significant ROI of SOAR for every organization that knows how to utilize its amazing powers.

People shouldn't mistake SOAR for some magical tool that replaces every other technology in the cyber security industry. Yet, SOAR should be understood as the binding force that connects the dots in a SOC environment and improves the potential of every tool it interacts with.

Do all SOAR Vendors Offer a SOAR Solution With the Same Quality?

One thing that everyone who is interested in SOAR should understand is that not every SOAR solution is the same. Different SOAR vendors build their SOAR solutions with different philosophies in mind. While most SOAR solutions contain the basics that every SOAR should provide (automation, orchestration, etc.), there are many differences among SOAR vendors, just as there is any industry where a product has grown in popularity and demand.

Some SOAR vendors may provide the bare minimum, while others go the distance and pave the way for the next-gen SOAR industry. DFLabs falls into the second category, and with three patents in the SOAR industry (the most out of any SOAR vendor) and many proprietary capabilities that are unique only to IncMan, DFLabs is dedicated to shaping IncMan SOAR into the best SOAR solution on the market.

While it is smart to hire the best security professionals on the market, if their potential is not optimally utilized with the help of contemporary technologies such as SOAR, you will end up paying thousands of dollars for your security professionals to drown in threat investigation alone due to the thousands of alerts an average organization is receiving.

How to Distinguish the Best SOAR Solution for Your Needs?

Choosing the right SOAR solution that perfectly aligns with your needs is not an easy task. You need to do your fair share of research because what worked for one client doesn't necessarily mean the same SOAR solution will work for you.

What you need to do to find the ideal SOAR solution is this:

- **Assess your needs:** The strengths of one SOAR vendor may not be applicable to your current use case, which is why you must investigate the need of your organization and find a SOAR solution that responds to those needs.
- **Make sure they have good customer support:** A quality SOAR vendor always puts client satisfaction as a priority. Which is why having a good customer support system is a trait of a quality SOAR vendor.
- **Customizability and flexibility:** It is always a good idea to choose a SOAR solution that prides itself on customizability and flexibility (such as our IncMan SOAR). A quality SOAR solution will allow you to integrate seamlessly with other security tools and offer an intuitive user interface.

Granted there are not one-size-fits-all SOAR solutions, but a flexible SOAR solution has a better chance of blending in almost every type of SOC environment.

Investing in a Strong SOC Team Without SOAR Will Downgrade Your ROI.

Prior to purchasing a SOAR solution, you will probably consider the pros and cons of investing in a SOAR solution. And while you do that, consider the structure of your organization. Now, the typical SOC team that any serious company should strive towards building mainly consists of:

- **Information Security Manager:** Average yearly salary is $51,881
- **Security analysts:** Average yearly salary is $76,410
- **Security engineers:** Average yearly salary is $99,834
- **CISO:** Average yearly salary is $179.539

The average salary for each of the aforementioned security professionals may vary depending on many variables (Country of residence, level of expertise, etc.c). Still, investing in a solid SOC team comes at a hefty price, nonetheless.

Furthermore, while it is smart to hire the best security professionals on the market, if their potential is not optimally utilized with the help of contemporary technologies such as SOAR, you will end up paying thousands of dollars for your security professionals to drown in threat investigation alone due to the thousands of alerts an average organization is receiving. This means that you'll be investing a mind-boggling amount of money in threat investigation alone, while threat remediation is still an unresolved topic. And you wouldn't want to spend a fortune on building a compact SOC team and not invest in the last piece of the puzzle that will bring harmony to your entire security operations center.

Your SOC team may work tirelessly to keep all your systems, data, and employees secured, but the more they are bombarded with huge volumes of data, applications, and tools to handle, the harder it becomes for them to effectively carry out effective SecOps. This is where SOAR comes into play as a connective tissue and force multiplier.

SOAR relies on a machine learning engine that constantly learns from the environment it is deployed, and the best part is that SOAR actually leverages the information from SIEM by extracting the data from processed alerts and performing accurate threat-detection predictions that help analysts have the upper hand over alerts as they arrive in real-time.

Why Investing in a SOAR Solution Pays Off?

Understanding how a SOAR platform helps your SecOps exactly is crucial.

SOAR actually makes your investment worthwhile because it affects the performance of your SOC in different ways:

- **Improves collaboration:** Your security professionals will have a tough time juggling multiple tools and dealing with thousands of alerts at once. By offering a customizable dashboard and automating a wide range of SecOps, SOAR helps bring your whole SOC team closer.
- **Freeing up time for analysts:** SOAR allows you to automate entire SecOps processes and fully automates a variety of low-risk assignments, thus freeing up time for your analysts to be more organized and productive.
- **Detecting false positives:** Many organizations struggle with huge volumes of alerts that have to be assessed by their analysts. And without a SOAR solution, the analysts will have to manually assess all the alerts, which is incredibly time-consuming and often leads to alert fatigue, and eventually, in loss of quality security professionals.
- **Retain valued security professionals:** The growing skill-shortage in the cyber world is making it hard to find decent security professionals and even harder to retain them. This is because the workload can sometimes be overwhelming, and when you add the fact that without SOAR, many security professionals will be delegated the responsibility of manually assessing every alert, it is understandable why the skill shortage is occurring in the first place.

SOAR helps you retain your security employees by doing the "boring part" of assessing every low-risk by implementing full or semi-automated actions. This allows your security professionals to have more time to focus on higher-risk assignments, which, in all honesty, are more challenging for your analysts.

Additionally, SOAR allows you to make the most out of your existing tools and technologies as well. For instance, pairing SOAR with your SIEM solution will drastically improve your SOC performance. Why? That's because SIEM itself is not able to distinguish between true and false positives. SIEM is an advanced alert-detection system that is able to detect alerts but is not capable of assessing their credibility.

This has to be done manually, by analysts and engineers. And constantly tweaking SIEM to be able to accurately determine the severity of a certain alert is a time-consuming process. But, with the implementation of SOAR, your analysts will no longer have to tweak SIEM. SOAR relies on a machine learning engine that constantly learns from the environment it is deployed, and the best part is that SOAR actually leverages the information from SIEM by extracting the data from processed alerts and performing accurate threat-detection predictions that help analysts have the upper hand over alerts as they arrive in real-time.

In other words, SOAR improves the functionality of every tool it interacts with thanks to its machine learning capabilities. This holds true for IncMan SOAR, in particular, thanks to its progressive OIF (Open Integration Framework) capabilities, allowing IncMan SOAR to connect with hundreds of the most popular technologies and apply over 1200 orchestrated actions in the process, ultimately improving the efficiency of the entire SOC team.

If your SOC team is overwhelmed with alerts, and if your SOC team is not expansive enough to deal with the tremendous load of too many alerts, then SOAR is definitely a technology worth investing in.

Evaluate the Needs of Your Organization.

Once again, let's emphasize the fact that investing in a SOAR solution should be contemplated in a meticulous manner. The best way to get the perfect ROI of your SOAR platform is to think about the needs of your organizations first:

- How many team members does your SOC team consist of?
- How many alerts do you receive on a daily or weekly basis?
- What are the most common types of cyber threats you receive?
- How important is fast incident response time for your organization?

Answering these questions is a must if you want your investment in a SOAR solution to be a productive one. SOAR's strengths lay in connecting a complex environment and untangling the process of having to through too many tools and alerts. So if your SOC team doesn't receive too many tools, is not that big, and if you commonly receive threats that are not that dangerous, to begin with, then you won't be able to extract the benefits of SOAR.

However, if your SOC team is overwhelmed with alerts, and if your SOC team is not expansive enough to deal with the tremendous load of too many alerts, then SOAR is definitely a technology worth investing in.

In short, SOAR will help you do more with fewer resources. And that's the biggest ROI you can ask for.

Learn how to Utilize SOAR’s Strengths.

As we mentioned before, SOAR's strengths lay in connecting people and drastically increasing the effectiveness of your SOC team. And yes, if used properly, SOAR can do wonders for your SecOps:

- Improves the effectiveness of your SOC team by 10 times
- Increases your incident response time by 80x
- Increases the number of resolved incidents by 300%
- Drastically improves threat hunting capabilities

However, these benefits don't come by default with the sole fact of implementing SOAR into your security ecosystem. After all, your security professionals are the ones that are going to be responsible for eliminating cyber threats; SOAR is just going to make their job a whole lot easier.

SOAR relies on a series of orchestrated actions that are designed to intercept cyber threats before they become full-blown alerts.

Let's face it, sorting through thousands of low-risk alerts is a mind-numbing job, and while your security professionals focus on sorting out the false positives, the real threats can slip away and do horrendous damage to your organization. Which is exactly why SOAR is such an integral aspect of every modern SOC team, as it drastically improves your incident response time.

SOAR learns repetitive patterns and can be instructed to fully carry out the SecOps process or only apply semi-automation. The degree of automation is adjustable and can be altered by your SOC team. That's the beauty of it. Given that many fear the incorporation of automation in cyber security processes, SOAR's fully adjustable automation proves there is nothing to be afraid of, as security automation only serves to boost the effectiveness of SecOps, not compromise them.

SOAR learns repetitive patterns and can be instructed to fully carry out the SecOps process or only apply semi-automation. The degree of automation is adjustable and can be altered by your SOC team. That’s the beauty of it.

Choose the Right SOAR Solution: What Makes IncMan SOAR the Best.

To make the most out of a SOAR solution, you need to make sure you've made the right pick. Not every SOAR solution provides the same features. While there are some standard features like orchestration and automation, many SOAR solutions differ due to their unique internal vision which is distinctive to every company.

There are those SOAR solutions that are deemed as pioneers in the SOAR industry, such as IncMan SOAR, and there are those who follow.

You need to choose a SOAR solution that puts the client's need in mind and is dedicated to always pushing toward innovation. The reason why SOAR is deemed as such an important aspect of cyber security is that SOAR is thought to be on the same level of sophistication as the most advanced cyber threats of today. But not all SOAR solutions are developed in the same way.

This is why you need to look for the clear tell-tale signs that speak silent volumes of the credibility of a certain SOAR vendor. For instance, when you look at what IncMan SOAR has achieved in the cyber security world, it is clear that IncMan belongs to the group of "pioneering" SOAR solutions:

- The SOAR vendor with the highest number of patents (Three)
- Protagonist of the OIF (Open Integration Framework) philosophy
- The only SOAR solution with OT/IT use cases

And most important of all, IncMan SOAR includes excellent customer support service, which will never leave you high and dry in times of need.

The reason why SOAR is deemed as such an important aspect of cyber security is that SOAR is thought to be on the same level of sophistication as the most advanced cyber threats of today. But not all SOAR solutions are developed in the same way.

Is SOAR Just for Large Organizations or It Is Also for Small and Medium Enterprises?

Generally speaking, SOAR is deemed to be suitable for larger organizations and structures companies that have established SOC environments with multiple employees. And to some extent, that statement is not far from the truth. SOAR does blend in well in complex environments where it acts as a force multiplier and a connective tissue.

One of SOAR's biggest strengths is to ease the burden of security professionals by automating a wide range of repetitive and manual tasks. On the other hand, taking into consideration the fact that small and medium organizations (and MSSPs as well) are also in need of SOAR, we created a scalable model that offers smaller organizations the same benefits as our conventional IncMan SOAR solution.

Ergo, we provide every type of organization access to the most open platform on the market.

Conclusion.

In this white paper, we discussed some of the most fundamental aspects of the SOAR technology. We took a closer look at how SOAR operates, as a distinctly novel technology, how it is different from SIEM, and how SAOR fits into the entire cyber security puzzle of modern SOCs.

We delved into the SOAR ROI and explained what SOAR brings to the table and why it is considered a vital asset of every high-functioning SOC, and we placed a special emphasis on security automation and its invaluable contributions to next-gen security operations.

And lastly, we unraveled the key differentiators of our own SOAR product - IncMan SOAR, and we explained just why IncMan SOAR is considered a pioneer in the SOAR technology.

With some of the most commonly asked questions in mind, we devise this white paper with the sole purpose of depicting every uncertainty you might have had about SOAR. And if you're still reading this now, we're sure those uncertainties are no longer present.

Automate.
Orchestrate.
Measure.

About Us.

DFLabs is an award-winning and recognized global leader in Security Orchestration, Automation and Response (SOAR) technology.

Its pioneering purpose-built platform, IncMan SOAR, is designed to manage, measure and orchestrate security operations tasks, including security incident qualification, triage and escalation, threat hunting & investigation and threat containment.

IncMan SOAR harnesses machine learning and automation capabilities to augment human analysts to maximize the effectiveness and efficiency of security operations teams, reducing the time from breach discovery to resolution and increasing the return on investment for existing security technologies.

As its flagship product, IncMan SOAR has been adopted by Fortune 500 and Global 2000 organizations worldwide.

The company's management team has helped shape the cyber security industry, which includes co-editing several industry standards such as ISO 27043 and ISO 30121.

DFLabs has operations in Europe, North America and EMEA.

For more information, visit our website www.dflabs.com or connect with us on Twitter @DFLabs.

DFLABS.COM

CONTACT US:

BOSTON - UNITED STATES
150 State Street
Boston, 02109
E - sales@dflabs.com

LONDON - UNITED KINGDOM
1 Primrose Street
London, EC2A 2EX
T - +44 203 286 4193
E - sales@dflabs.com

MILAN - ITALY
Via Bergognone, 31
20144, Milan
T - +39 0373 82416
E - sales@dflabs.com

CUSTOMER SUPPORT

T – +39 0373 82416
E – support@dflabs.com

Automate.
Orchestrate.
Measure.