SPONSORED BY

KnowBe4
Human error. Conquered.

Buyer's Guide:

Using SOAR in Your Automated Incident Response Plan

ebook
An SC Media publication

Learning to SOAR

End users report emails they think could be malicious, resulting in a lot of alert noise security teams must analyze. The question: how to effectively manage the volume of traffic and stop email threats that are truly malicious from reaching your employees' mailboxes in the first place? A Security Orchestration, Automation and Response (SOAR) platform will help, but buyers need a roadmap to determine requirements, vet SOAR providers and properly plan deployments. ***Paul Wagenseil*** *walks buyers through the process, using KnowBe4's PhishER platform as an example.*

OUR EXPERTS: Security Orchestration, Automation and Response (SOAR)

Chris Cline
Vice President of Product Management, KnowBe4

Brandon Smith
Product Manager, KnowBe4

Jacob Ansari
PCI Practice Leader, Mazar, U.S.

Frank Kim
CISO-in-Residence, YL Ventures

Adam "Sully" Perella
Manager, Schellman

The sheer number of events an organization's security team must keep up with can bog down even the most productive staffers. A Security Orchestration, Automation and Response (SOAR) platform lightens the load by automatically responding to events, taking immediate steps to remediate issues and alerting the necessary personnel.

But a SOAR platform is no magic bullet and it won't solve all your security issues. It can be complicated to set up, and your staff may take months to learn to use it properly.

"For even modestly complex organizations, actually realizing the full value of these tools takes some time and effort, and adopters of SOAR tools should not expect overnight transformation," says Jacob Ansari, PCI practice leader for the U.S. division of Mazars, an audit, tax and advisory firm.

Here's what SOAR can and can't do, how to prepare your organization to use it and how to select the proper SOAR platform:

What SOAR is and how it can help

SOAR is the next step in the evolution of security information and event management (SIEM), a class of meta-tools that aggregate data from disparate security programs and present them to security analysts in one place.

Both SIEM and SOAR collect incident data. The difference is that while SIEM is passive, SOAR is active. A SIEM tool will issue a report or alert and then leave it to human staffers to act. A SOAR tool will use the information gathered to automatically act without waiting for human intervention.

"In the current [SIEM] model, even if you have staff, an alert comes in and then they begin to do their triage and analysis," says Adam "Sully" Perella, manager at Schellman. "The idea of SOAR takes all of those manual operations and provides immediate response. You don't have the delay that can allow an infection to spread or an attack to go on."

You won't be turning over your organization's security to robots, however. SOAR uses human-created "playbooks" to respond to predictable events with predetermined actions.

> ***"For even modestly complex organizations, actually realizing the full value of these tools takes some time and effort, and adopters of SOAR tools should not expect overnight transformation."***
>
> - Jacob Ansari | *PCI Practice Leader, Mazars in the U.S.*

A SOAR playbook can make sure an endpoint machine is taken offline if malware is detected or help your incident response team identify email threats that made it past your email filters into your users' mailboxes. For example, KnowBe4's PhishER platform can automatically prioritize, quarantine and dispose of email messages based on rules you set as part of your security workflow.

"PhishER is helping you figure out whether something is good, bad or indifferent and [determining] what to tell your users. The thing that makes PhishER special is that it lives after all the other technical controls you've got fail," says Chris Cline, vice president of product management at KnowBe4.

Cline explains that unlike other SOAR platforms that sort through incoming email messages and use artificial intelligence to determine which emails might be malicious, PhishER takes the opposite approach: It starts with messages that humans have already flagged as suspicious and uses them to train its AI, called PhishML.

"Most email is not malicious by design," says Cline. "Then a human looks at the email and thinks, maybe this is malicious and reports it as a threat. This type of action goes into PhishML's feedback loop continually training the model. Every single piece of data that we feed our PhishML has already bypassed every layer of defense in depth that an organization has and [was] caught by a human."

Multiple SOAR playbooks can be chained together to create more complex responses to incidents. And because SOAR acts almost immediately, it shrinks an organization's mean time to respond (MTTR) to threats.

"SIEM offers many out-of-the-box, automated responses for performing mundane tasks related to [incident response], but certainly not to the same level as SOAR," says YL Ventures CISO-in-Residence Frank Kim. "SOAR is often far more useful in actually moving forward with security events via a wider arsenal of automated offerings and tooling."

SOAR also handles mundane tasks like creating and sending tickets, logging data and alerting designated personnel. After taking routine actions in response to commonplace events and taking care of a lot of the paperwork, a good SOAR platform frees up human staffers to handle more complicated and urgent tasks.

> ***"SOAR is often far more useful in actually moving forward with security events via a wider arsenal of automated offerings and tooling."***
>
> - Frank Kim | *CISO in Residence, YL Ventures*

SOAR tools require quite a bit of work to set up because each organization must tailor their playbooks and deployments to existing environments, tools, security policies and processes. Before deciding to install a SOAR platform, an organization should inventory its assets, assess its needs and calculate the cost of implementation in fees and work hours.

"It's very easy to sell someone something when they're terrified of becoming the next victim of a ransomware attack," says Perella. "You need to do your due diligence. You're going to invest, not just the upfront cost of the service, but also all of the man-hours. You need to see whether this will have a demonstrable return."

That fine-tuning is also a SOAR platform's strength. If the tool is properly set up, it can fit the client organization perfectly.

"[PhishER is] extremely customizable. We let admins choose what to do," explains Brandon Smith, a product manager at KnowBe4. "[Our platform] is only trained on reported messages that humans say are malicious [so that] you can determine what is a threat."

How SOAR works

Like a SIEM tool, a SOAR platform collects data from dozens of security tools dispersed throughout an organization, such as endpoint protection solutions, intrusion detection and protection (IDS/IPS) and data-loss prevention (DLP) systems, vulnerability scanners and email and web protection systems. SOAR tools can also use external threat intelligence feeds and gather data from SIEM tools themselves.

Unlike a SIEM tool, which ingests a one-way data feed and presents its conclusions to humans, a SOAR platform orchestrates the actions of security tools and communicates with them, querying them for information, if it spots a pattern of widespread intrusion, and commands the tools to respond accordingly. A SOAR platform integrates the actions of tools into its own activity, coordinating them to work in concert like a conductor leading an orchestra.

"In a world of certainty, you can get resilience through automation. In a world of uncertainty, you get resilience through orchestration," information-security expert Bruce Schneier noted, during an RSA Conference keynote address in 2019. "Incident response is inherently uncertain, and that makes it hard to automate."

SOAR tools can detect patterns in repeated events and create new playbooks to respond to them, cutting down response times without letting problems fester. They can also suggest other responses that humans can authorize. By consolidating all security activity and putting it into context in a single dashboard interface, they let staffers make decisions more quickly.

> ***"In many cases, these are complementary tools. SIEM is helpful in collecting and analyzing event data and yielding alerts or notifications, and SOAR can help automate and streamline the response effort where many organizations are lacking."***
>
> - Jacob Ansari | *PCI Practice Leader, Mazars U.S.*

However, a SOAR tool is not meant to replace other security tools — even SIEM tools. Instead, SOAR ties all the tools together and augments the activities of those tools, just as it augments the activities of SOC staff.

"In many cases, these are complementary tools," Ansari says. "SIEM is helpful in collecting and analyzing event data and yielding alerts or notifications, and SOAR can help automate and streamline the response effort where many organizations are lacking.

"But it's rare that one suite of applications does everything very well," he adds, "and far more likely that integrations between different tool sets yield the most success for the widest spread of organizations."

There's also the danger that, as with many security platforms, an organization might expect too much from a SOAR tool. It will not fix all your security problems, and it cannot replace your security staff. But, if it is properly configured and used, SOAR will make your security responses faster and more efficient.

"The people implementing SOAR may be over-relying on it," Perella says. "The core elements of information security still need to be applied." SOAR tooling cannot necessarily resolve certain endemic problems like an inability to identify assets added to corporate networks or shadow IT efforts connecting new third-party applications to a network, Ansari says, adding, "These tools can maybe help define the scope of the problem or alert a team to when such an occurrence happens, but may also be blind to such happenings, depending on the implementation."

Cline points out that as good as PhishER is at defeating malicious emails, the ultimate protection still must be provided by a well-trained end user.

"If you're looking to handle email, we can help automate your response — but we're not the answer," he says. "The Verizon DBIR [Data Breach Investigations Report] says email is the vector for 85% of breaches. You can't ignore that. If you're not training the end user, you're leaving open the biggest door into your organization. If you're not managing that, you're letting a lot in."

Does your organization need SOAR

Every organization can use help responding to routine security events. The question is whether implementing a SOAR platform will yield cost benefits, considering the price and the work-hours required to set it up and use it properly.

The first things to do are to identify the gaps in your current security tools to find out which of those tools can be automated by a SOAR platform, and to inventory your assets. Ask yourself: How well do your existing tools work with each other? How much can be automated with the technology you already have? How many of your assets are on-premises and how many are in the cloud?

"I recommend thinking about the skillset of the people on your team, the processes you currently have and the tech you currently have," says Kim. "Then, identify what your gaps are and where automation can actually help. This is how you can determine which workflows and processes will give you the best bang for your buck."

It might be the case that you need SOAR to protect only certain aspects of your environment, such as web access or email. In those cases, specialized tools with SOAR capabilities, such as KnowBe4's PhishER platform, may be enough.

"We don't want to be the SOAR for everything. We want to be a focused SOAR that handles email better than anyone," says KnowBe4's Cline. "If you think you have a real need for a SOAR, you're probably oversimplifying things with your expectations, or you're overcomplicating things by adding yet another vendor."

While PhishER's use case can be extended to protect other systems, it might not work as well as more general SOAR platforms. Nor might general SOAR platforms be as efficient at handling email threats.

"We call [PhishER] a lightweight SOAR," says Cline. "You can create a giant playlist inside of [a SOAR platform for email related threats] and have it handle most of what PhishER does. But I talked to people and the answer was 'Yes, you can do it in a SOAR, but I've got at least one full-time employee on it,' and most of the time it's three or four employees. All the steps you need to respond to email threats are wildly easier with PhishER."

With PhishER, attachments and URLs from user-reported emails are automatically scanned; setting up canned responses to your users is easy and you can escalate certain categories of messages to specific SOC teams with minimal setup.

An organization's security team also needs to be mature enough to use SOAR efficiently and to recognize its strengths and shortcomings. You can't just install SOAR and flip a switch.

"The time it takes to learn how to use a SOAR platform is directly dependent on the maturity of the team using it," says Kim. "If you already have well-defined processes, you're looking at a quicker ramp-up time. It will naturally take longer if you need to develop your own requirements and processes from scratch."

Any SOAR platform you choose will likely have a steep learning curve, and its overall cost-effectiveness may partly depend on whether it takes your team three weeks or three months to learn how to use it properly. You need to be willing to invest a substantial amount of time to deploy a SOAR tool, master its use and build new playbooks and integrations.

While you consider SOAR platforms, ask around your industry to see what other organizations have chosen and what their experiences have been. Some SOAR providers might charge a lot to add functions or to aid with integration, while others might not offer much help at all.

> ***"If you're not training the end user, you're leaving open the biggest door into your organization."***
>
> - Chris Cline | *Vice President of Product Management, KnowBe4*

You can ask potential SOAR vendors for customer testimonials, inquire about the level and cost of post-purchase support and ask what kind of new features and functions they might be working on. A SOAR provider that doesn't innovate might quickly fall behind.

What to look for in a SOAR platform

No two SOAR deployments can be implemented the same way, as each organization must tailor SOAR to suit its own requirements.

"Plan for an extensive effort in implementation," Ansari says. "Try to get some fundamentals, like asset management, working first, even if they're manual and labor intensive, because SOAR will help automate that but won't fix problems like too many procurement processes."

There are certain fundamental aspects to look for, and questions to ask, when shopping around for SOAR:

A starter set of playbooks:
Does the SOAR platform come with a rich set of pre-built playbooks that can respond to the most common threats and incidents immediately after deployment? PhishER's default "System Rules" and PhishML make categorizing emails a breeze, right from the start.

A starter set of integrations:
Is the SOAR platform equipped to interface with widely-used enterprise security tools?

Ease of use:
How easy is it to understand the information that the SOAR platform puts forward and the workflows it creates? And how much work does the SOAR platform take off human hands?

Customizable dashboard:
How much information can be displayed on a single dashboard? To what extent can your team decide what goes there?

Simple playbook creation:
SOAR should ideally offer a no-code or low-code modular presentation so that anyone can build a new playbook.

Editable source code view for playbooks:
Some skilled security personnel might want to drop into the source code, and the SOAR platform should let them do so easily.

Artificial intelligence/machine learning:
How well is the SOAR tool able to learn from experience and improve its responses and playbooks? KnowBe4's PhishER analyzes user-tagged phishing and spam messages to better recognize email threats, then flips the malicious messages around and uses them for training purposes.

Bidirectional APIs and webhooks:
A SOAR platform should easily integrate with your current and future tools, regardless of which vendors they come from. SOAR ideally adapts to your existing environment. Your environment shouldn't have to be reshaped to fit SOAR.

Case and incident management:
Is the SOAR platform smart enough to recognize different events as part of a single case, and to present the case to analysts as such? PhishER's Rooms feature automatically groups similar messages, allowing you instant economies of scale.

Human supervision:
How easy is it to customize playbooks and responses so that human approval is needed for certain tasks to be carried out by the SOAR platform?

Threat intelligence:
Can the SOAR platform ingest and use a constant feed of threat intelligence from outside the organization? For example, KnowBe4's PhishER integrates a feed from VirusTotal.

Pricing:
There are three prevalent pricing models for SOAR platforms: You can pay for each action taken or automation enabled; you can pay per endpoint or node; or you can pay a flat subscription fee, sometimes with additional costs for each admin account. The flat fee may be the simplest and most appealing, but you might save money with one of the other two models.

Long-term vendor support:
Will the vendor update the software at no additional cost? Will the vendor create and supply new playbooks? Will the vendor help you on-demand, such as when you need to have a custom integration with a new piece of software?

Conclusion

This buyer's guide to Using SOAR in Your Automated Incident Response Plan has offered insights into the what, how, and why of SOAR for incident response. A SOAR platform can help shrink an organization's mean time to respond [MTTR] when responding to threats.

Phishing remains the most widely used cyberattack vector and creates a volume problem for your incident response team. Platforms like KnowBe4 PhishER help you identify and respond to dangerous email threats faster. It's a key ingredient of an essential security workstream to orchestrate your threat response and manage the high volume of potentially malicious emails reported by your users.

SPONSORED BY

KnowBe4
Human error. Conquered.

About KnowBe4's PhishER

PhishER is a simple and easy-to-use lightweight Security Orchestration, Automation and Response (SOAR) platform that helps orchestrate your threat response and manage the high volume of potentially malicious email messages reported by your users. And, with automatic prioritization of emails, PhishER helps your InfoSec and Security Operations team cut through the inbox noise and respond to the most dangerous threats more quickly. Incident response orchestration can easily deliver immediate efficiencies to a security team. With the right strategy and planning, an organization can build a fully orchestrated and intelligent SOC that can contend with today's threats. PhishER is a critical element to help incident response teams work together to mitigate the phishing threat.

For more information, please visit www.knowbe4.com/products/phisher

MASTHEAD

EDITORIAL

VP OF CONTENT STRATEGY

Bill Brenner | bill.brenner@cyberriskalliance.com

PROJECT MANAGER

Victor Thomas | victor.thomas@cyberriskalliance.com

SALES

CHIEF REVENUE OFFICER

Dave Kaye | dave.kaye@cyberriskalliance.com

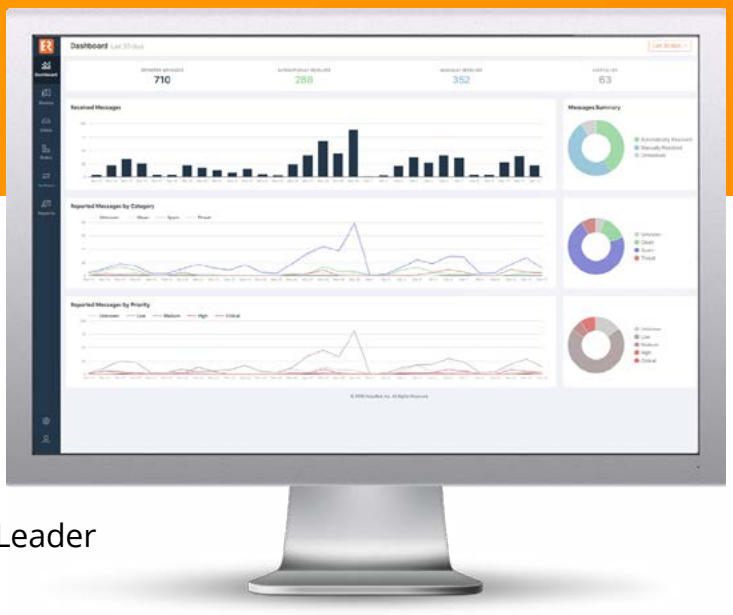
DIRECTOR, STRATEGIC ACCOUNTS

Michele Guido | michele.guido@cyberriskalliance.com

PhishER

Identify and Respond to Email Threats Faster

Request a Demo »



Cut Through Inbox Noise To Stop Phishing Emails In Their Tracks With PhishER

Sign up for a 1:1 demo of PhishER, the #1 Leader in the G2 Grid Report for SOAR Software.

- **Automate message prioritization** into one of three categories: Clean, Spam or Threat
- **Search, find, and remove email threats with PhishRIP**, PhishER's email quarantine feature
- Automatically **flip active phishing attacks into safe, simulated phishing campaigns** with PhishFlip
- **Integration with KnowBe4's email add-in button, Phish Alert,** or forwarding to a mailbox works too
- **Unlock Incident Response resources** by managing the 90% of messages that are spam or legitimate

Request your demo here: https://info.knowbe4.com/phisher-request-a-demo-sc

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com