KnowBe4
Human error. Conquered.

8 Essential Capabilities When Evaluating SOAR Platforms

Enhancing security awareness should always be the top priority for organizations looking to improve their defenses against phishing. But as cybercriminals continue to refine their tactics, the need for a robust, comprehensive phishing defense strategy has become paramount. Security operation center (SOC) and incident response (IR) teams need tools that allow them to rapidly investigate and terminate phishing attacks before they can inflict damage.

This is why anti-phishing Security, Orchestration, Automation and Response (SOAR) products have emerged as powerful tools in the battle against phishing, offering a unified approach that combines technology and human expertise. They are now a critical component for IT security pros looking to counter the expanding threat landscape of phishing attacks and targeted spear phishing campaigns.

But not all SOAR products are created equal. First and foremost, a good SOAR product should automate the analysis and prioritization of truly malicious emails to eliminate the guesswork of identifying high-risk phishing threats. Moreover, during the past several years, additional powerful features have allowed SOAR products to go from reactive analysis and identification to proactive phishing mitigation. Understanding these capabilities and advancements is important as you assess the marketplace.

When it comes time to select a SOAR product for your organization's anti-phishing defense, here are the eight capabilities you should prioritize.

#1 EMPOWER YOUR END USERS

The cornerstone of an organization's defense against phishing and social engineering threats is its end users. Their ability to identify and report cyber threats is the foundation for your organization to safeguard itself from phishing attacks and to reduce the risk they present. A good SOAR product should empower your end users to accomplish this.

First, the ability for end users to easily report suspicious emails. A phish alert button, which is embedded within your organization's email client, should allow users to report suspicious emails to a pre-designated IT inbox or directly into the SOAR platform.

Second, a SOAR product should include templates and automated email responses to allow your infosec team to quickly communicate back to employees about emails they've reported and whether those reported emails were in fact just spam or actually clean—90% of the total traffic.

#2 MACHINE LEARNING & AI

Powerful phishing protection is enabled by a SOAR platform that leverages artificial intelligence (AI) and automation. Under-staffed IR and SOC teams can't go it alone, and AI and automation acts as a force multiplier for making the identification and prioritization of phishing threats easier, faster and more accurate.

AI and automation will both enable and dramatically speed up the following capabilities listed because they provide scalability, accuracy and proactive mitigation:

- Automatic analysis and prioritization of emails to eliminate the guesswork of identifying high-risk phishing threats from all the user-reported messages

- Automate the security workstream for managing the “other 90%” of user-reported emails
- Automated email responses to allow IT to quickly communicate with employees
- Group or cluster messages based on machine learning pattern recognition to allow incident response teams to identify a widespread phishing attack
- Automated blocklisting, crowdsourced threat intelligence and proactive phishing mitigation
- The ability to take real-world phishing attacks and change them into simulated phishing templates to train your employees

#3 AUTOMATED THREAT ANALYSIS AND PRIORITIZATION

Many IR and SOC teams still rely on manual workflows to triage a suspicious email. On average, it takes 27 minutes to manually triage a phishing email.[1] A poor mean time to respond increases the risk and potential damages from a phishing attack.

To safeguard your organization effectively and maintain your security team’s sanity, implement a SOAR product that leverages machine learning-powered analysis and prioritization of emails. This eliminates the guesswork in identifying high-risk phishing threats from the firehose of user-reported emails.

Ensure any product you’re evaluating leverages machine learning to automatically prioritize reported emails without human interaction. This should include categorizing emails into various categories, such as Clean, Spam or a Threat, and rank suspicious emails based on priority by analyzing an array of email attributes, such as subject, sender, recipient, attachments, body copy, etc.

Like any good machine-learning platform, it should learn as well. As new data is fed into the system, such as suspicious emails reported by your end users, data from your SOC team, or verified threat information by a third-party threat intelligence feed, its accuracy should constantly improve, thereby allowing it to automatically prioritize more emails, more accurately.

Email analysis and prioritization is the foundation for any good SOAR product and will make the prioritization of emails easier, faster and more accurate.

---

1 The Business Cost of Phishing, 2022 Report

#4 QUARANTINE AND REMOVAL

Once a phishing threat is identified, capabilities to quarantine and remove similar phishing emails from all users' inboxes is paramount. In a world of nation state threat actors and targeted spear phishing attacks, this ability to mitigate phishing at scale is critical.

This email quarantine capability should directly integrate into third-party email services, such as Microsoft 365 or Google Workspace, and should enable you to:

- **Remove**
  Once the threat has been identified, your SOC team should have the option to remove the same or similar messages from all mail folders, whether it be inbox, sent, trash, etc.
- **Inoculate**
  Not all end users will report suspicious emails. For those that don't, you'll want the ability to monitor and detect those unreported emails so you can report, quarantine and eventually analyze.
- **Protect**
  Post-mortem analysis is vital to stopping the next attack. Once any immediate threats have been mitigated, capabilities to send follow-up communications to impact users, delete messages from your users' mailboxes, keep them quarantined, or restore messages that are identified as legitimate are all capabilities that should be on your checklist of key capabilities when evaluating a product.

#5 BLOCKLISTING

Blocklisting is the most fundamental, proactive approach to prevent malicious emails from reaching your users' inboxes. Email services such as Microsoft 365 and Google provide basic blocklisting functionality, but this is nowhere sufficient enough to stop today's array of AI-created phishing emails.

Any SOAR product you're evaluating should strengthen your organization's existing email filters by providing superior blocklisting capabilities that are driven by end user feedback and machine learning-based email analysis.

It should equip IR and SOC teams with the ability to block emails based on an array of attributes and values, such as sender, URL, attachments or file hash. Additionally, look for more robust condition-based rule creation functionality that supersedes the capabilities found in third-party email services.

Lastly, and perhaps most importantly, to stay ahead of the threat landscape and to proactively mitigate phishing attacks before they strike your organization, an enterprise-grade SOAR product should take blocklisting to another level by harnessing the power of AI and crowdsourced threat intelligence. Read #6 to understand why.

#6 CROWDSOURCED THREAT INTELLIGENCE AND PROACTIVE ANTI-PHISHING PROTECTION

Not even the largest, most well resourced SOC and IR teams can possibly stay ahead of the phishing/social engineering threat landscape. The threats are too diverse, constantly evolving and increasingly sophisticated. AI has empowered cybercriminals to create new phishing emails capable of evading traditional email security filters.

That's why in the world of phishing defense, being proactive is the name of the game. Any SOAR platform you implement should serve as a vigilant lookout, seamlessly integrating real-time threat intelligence data. This ensures that the latest insights about emerging threats are at your fingertips, empowering you to adapt and counter swiftly.

This is why organizations are increasingly relying on cybersecurity vendors as threat intelligence hubs. Your SOAR vendor should provide crowdsourced threat intelligence and AI-powered blocklisting to automatically quarantine and remove phishing threats from your users' inboxes based on verified real-world phishing threats that millions of other end users have already reported.

Crowdsourced threat intelligence sees the threats that made it through all other filters. It provides an additional layer of protection against the malicious emails that slip past secure email gateways and into your users' inboxes. According to ArmorBlox, 56% of email-based attacks bypassed legacy security filters in 2022 and 18.8% of phishing emails bypassed Microsoft Exchange Online Protection and Defender to make it to a user's inbox, according to a report by the Check Point Email Research Team.[2]

#7 CUSTOMIZABLE WORKFLOWS

Phishing analysis and mitigation isn't a one size fits all model. Workflows and processes will vary from one organization to another. Select a SOAR platform that offers the flexibility to mold automation workflows to your organization's unique needs. Whether it's analyzing suspicious emails, categorizing incidents or initiating predefined responses, customization is key.

---

2 Check Point Microsoft Defender Report

#8 TURN PHISHING ATTACKS INTO TRAINING

Many organizations want to test users on identifying and reporting phishing emails that closely resemble real-world threats. A SOAR product should make that super easy by providing the ability to "flip" a malicious phishing email into a real-world training opportunity for your users. This capability will also help reinforce your existing security awareness training program.

Email threats that have been reported and removed should be used to create a "defanged" version, then automatically initiate a simulated phishing campaign to users. This should include the ability to replace real phishing emails that made it into your users' inbox (but wasn't yet opened) with the "defanged" version, resulting in users that are more vigilant to real-world threats.

THE UPSHOT

In the battle to keep your organization up and running, the battle against phishing attacks requires a comprehensive strategy. SOAR tools, with their orchestration, automation and response capabilities, give you a formidable defense.

The marketplace for anti-phishing SOAR products is as diverse as the social engineering threats they're designed to mitigate. Ultimately, any SOAR product you implement should optimally reduce the mean time to respond and mitigate phishing threats before they make it into your users' inboxes, while supercharging your organization's existing email security defenses. It should shift the burden off your IT team onto AI-powered automation and crowdsourced threat intelligence so your security teams can focus on orchestration and analysis while reducing the risk that phishing presents to your organization.

KNOWBE4 PHISHER PLUS

PhishER Plus is a lightweight SOAR product designed to orchestrate your phishing threat response and supercharge your organization's email security defenses. PhishER Plus combines robust machine learning-powered email analysis, prioritization inoculation and blocklisting capabilities with the industry's most powerful global threat feed for proactive anti-phishing protection.

PhishER Plus is powered by a triple-validated, global threat feed that automatically blocks phishing attacks before they reach your users' inboxes. There are three critical components powering the PhishER Plus global threat feed:

1. KnowBe4's global network of 10+ million highly trained KnowBe4 end-users and their PhishER Administrators
2. PhishML, a unique AI-model trained on phishing emails that all other filters missed
3. Human-curated threat intel by KnowBe4's Threat Research Lab

Identify and respond to phishing threats faster with KnowBe4's PhishER Plus.

Learn More

Request a demo of KnowBe4's PhishER Plus.

Request Demo

Additional Resources

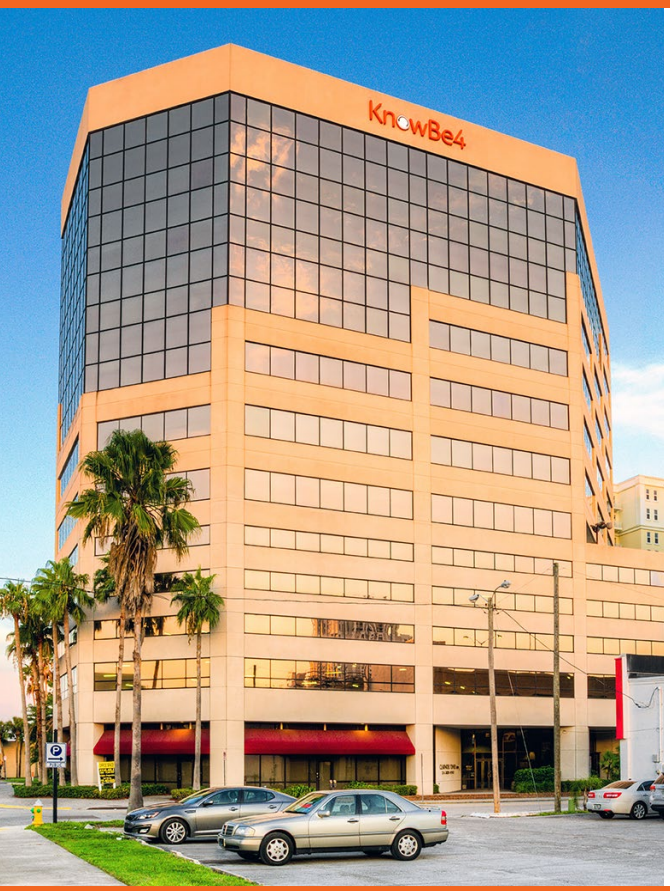
Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain



About KnowBe4

KnowBe4 is the provider of the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing attacks and enterprise-strength reporting to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

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

01D09K01