RAPID7

3 COMPONENTS OF AN EFFECTIVE ANTI-PHISHING STRATEGY

[And how to implement them to combat the most prevalent cyber threat.]

93%

PHISHING ATTACKS ARE BEHIND 93% OF ALL DATA BREACHES[1]

Phishing attacks are the #1 threat to businesses today, with email and social engineering being the most common methods of attack.[2]

You've hired the best employees and put up the right defenses, but one thing keeps slipping in the door: phishing emails. Part of doing business today, unfortunately, is dealing with phishing attacks, which can range from the opportunistic to the targeted attack. Your defense ultimately relies on how effective your users are at detecting phishing emails, links, and attachments. Attackers know this, which is why they've become quite savvy at duping users with believable pretext (e.g. sending an email from "the CEO") or a false sense of urgency (e.g. requesting a "mission-critical" expense be paid).

If even one user's account is compromised, an adversary can then send a legitimate corporate email to anyone in the company, which can magnify clicks and the risk of further breach.

However, a comprehensive anti-phishing program can be built with just three foundational elements—read on to learn more.

[1] 2018 Verizon Data Breach Investigations Report
[2] 2017 SANS Threat Landscape Survey

1 PROACTIVELY BLOCK MALICIOUS EMAILS

(ESPECIALLY THE OBVIOUS ONES)

While it's impossible to preemptively block **all** phishing attempts, it still makes sense to try and prevent the simple stuff.

Let's start with a given: Secure email gateways can reduce your exposure to commoditized, opportunistic phishing campaigns, and can also come with features to help identify data leakage and support compliance.

Next step, involve your users; make it easy for them to report a suspected phishing email to your team. If your users have an easy, seamless way to report a suspicious email or link, they'll be more likely to do so. Put a complicated reporting process in front of them, however, and the chances that they report it will drop to near-zero. (Ignorance is bliss, remember?)

This is where a **phishing reporting and analysis tool** can empower your users to report suspected phishes with a one-click button from right within their email clients.

2 IMPLEMENT USER AWARENESS TRAINING AND SIMULATIONS

When you combine phishing awareness and training with an easy way to act on that knowledge, you **empower users** to become your best security advocates.

Phishing is a human problem. To make your people more resilient, ensure that phishing awareness training is in place. This can be done through a two-step process: (1) user education, and then (2) simulated testing to assess user identification and reporting. Campaigns should be sent out shortly after training, and then periodically throughout the year—this keeps users on their toes, and gives you enough data points to measure long-term training effectiveness.

Over time, you'll be able to measure how your users are faring at phishing identification and reporting. If you send 100 simulated emails, are you getting 25, 50, or 75 percent more people reporting over time? Ideally you should see improvement, but if not, that may be a sign you need to revisit your training program.

With metrics in hand, you can demonstrate training progress to leadership, which can help validate training efforts and highlight improvement across the organization.

3 DETECT COMPROMISED USERS

It's inevitable that at some point, one of your users will fall for a phish... if they haven't already. In order to stop an attacker from accessing sensitive data, you need to know **who they duped** and **what happened.**

When investigating an incident, it's essential to know each step an attacker took across your user accounts, endpoints, and the internal network to ensure that remediation is thorough and avoid rebreach.

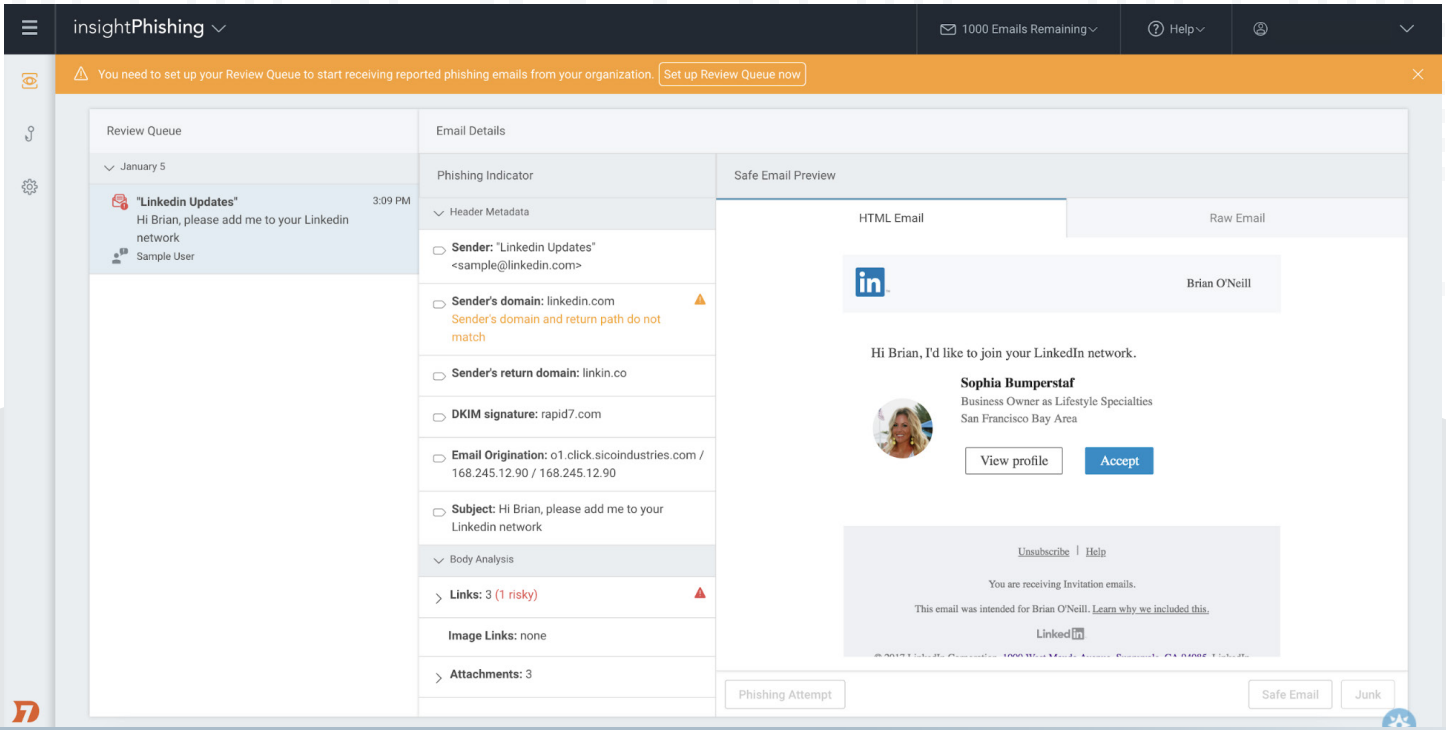
However, even with automated alerting, phishing investigations take too much manual effort, even if they're just to confirm that a suspected phishing email is benign. That's where **SIEM technology** comes in, giving you the network-wide visibility required to identify compromises across your environment, right down to the exact users with stolen credentials or assets with active malware.

Together, SIEM and phishing technology can provide you with a defense-in-depth approach.

HOW-TO

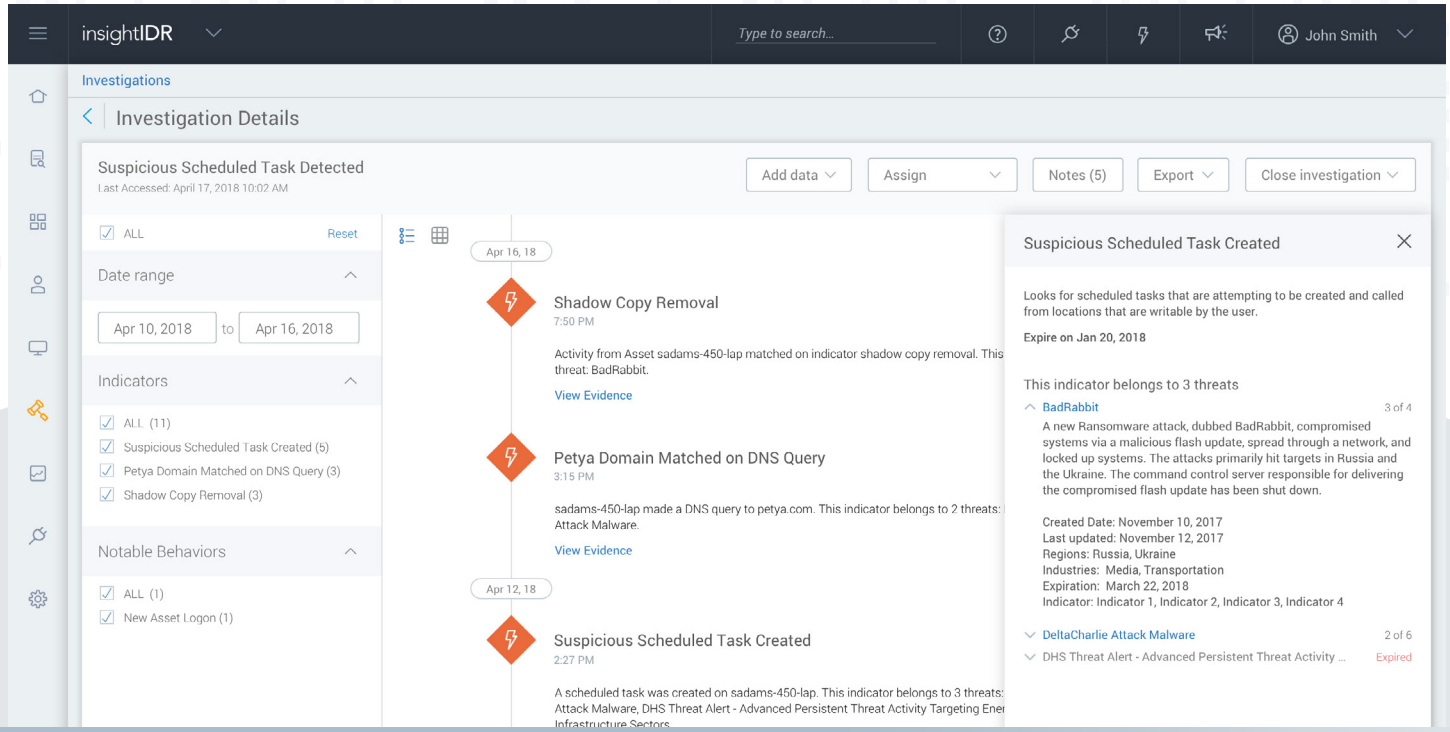
CREATE A DEFENSE-IN-DEPTH STRATEGY WITH RAPID7

Having the capability to identify compromised user accounts and credentials is the biggest challenge for nearly every company today. Fusing together user reporting with modern threat detections can give you complete end-to-end visibility.



Employee reporting is **the most common method** for discovering a breach. By using a tool like **InsightPhishing**, users can report suspected phishing emails with one click, directly from their inbox. You're provided the email's metadata and body content, which InsightPhishing automatically analyzes for suspicious indicators.

Any of these indicators can be added to a custom phishing indicator database for your organization so that your team can leverage findings from past investigations; the more you train InsightPhishing, the better it gets. If you identify a malicious phish, you can use a SIEM solution like **InsightIDR** to scope out affected users, gain additional context, and improve your defenses.



InsightIDR applies two layers of analytics to your data to find attacks: **User Behavior Analytics** (UBA) to identify users exhibiting behaviors indicative of compromise, and **Attacker Behavior Analytics** (ABA) to hunt the underlying techniques attackers use time and time again.

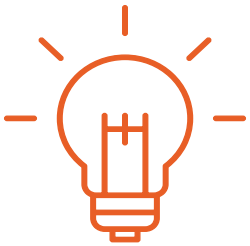
Any malicious URLs can be added to InsightIDR, which will then automatically match against future DNS, firewall, web proxy, and other user data. If a user accesses that URL in the future, InsightIDR will alert you and help you take swift action.

The key to preventing future compromise lies in translating your investigation findings into threat intelligence, and feeding that back into your proactive defenses.

When you're investigating an incident, you can always search across all of your logs with InsightIDR to identify other users that interacted with the URL. If an attacker sends a phishing email to the entire organization, you can quickly identify the exact users that clicked on it so you can take appropriate action (e.g. change a password or deprovision an account).

You'll also have context into notable user and asset behavior exhibited around the same time.

This could include the installation of new malware, unusual user account activity, new processes running, vulnerabilities exploited, and more to better inform remediation. This level of readily available context allows you to patch a vulnerability, shut down a process, or lock out an account to keep confidential assets and data safe.



LEARN MORE

about achieving a true defense-in-depth strategy with InsightPhishing and InsightIDR to secure your data and company from phishing attacks.

rapid7.com/try/anti-phishing

CONTACT US OR CONNECT WITH US

North America: +866.7.RAPID7 | sales@rapid7.com
EMEA: +44.(0)118.207.9300 | emeasales@rapid7.com
APAC: +65.3159.0080 | apacsales@rapid7.com

twitter.com/rapid7