AGARI

SOLUTION BRIEF

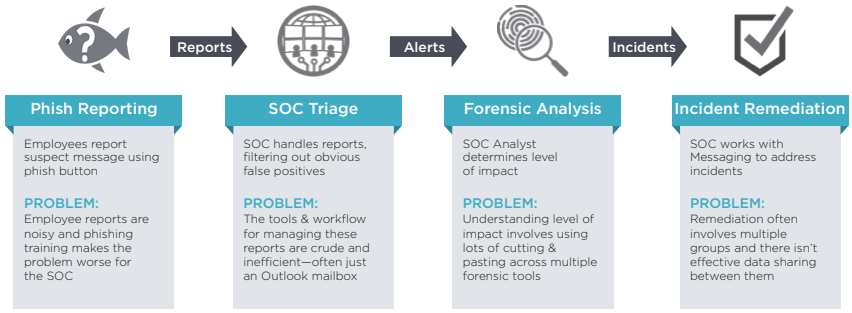
Agari Incident Response™

Accelerate phishing incident triage, forensics, remediation, and breach containment.

The Challenges of Phishing Incident Response

Phishing and other email-based attacks account for 96% of breaches[1], with cybercriminals exfiltrating data mere hours after gaining access. However, it often takes months for businesses to discover a breach—and even longer to remediate it.

Most employees are trained to report phishing and often have a convenient button or abuse inbox to forward messages to the security team. Employee reported phishing can be one of the best sources of breach threat intelligence and helps prevent or contain breaches. However, the unintended consequence of employee reporting is that Security Operations Center (SOC) analysts become overwhelmed by the sheer number of reported phishing incidents—the majority of which turn out to be false positives. Many organizations receive tens of thousands of phishing incident reports per year, requiring analysts to correlate data from five or more tools, sift through tedious email logs, and then manually remove emails one by one from inboxes.



> "Many organizations' security operations teams report their work around investigating suspected phishing emails is heavily repetitive and requires many meticulous steps, such as checking multiple blacklists and different IT systems within the company."
>
> Gartner Preparing Your Security Orchestration and Automation Tools (ID G00325580)

AT A GLANCE

Agari Incident Response™ is the only turnkey solution purpose-built for Microsoft Office 365 to automate the process of phishing incident response, remediation, and breach containment.

BENEFITS

Avoid financial losses by detecting breaches before they successfully compromise employees.

Save time for Security Operation Center (SOC) analysts by automating the process of incident response.

Automatically remediate similar phishing messages sent to multiple employees.

Quantify risk reduction and calculate savings with an intuitive executive dashboard.

THE AGARI ADVANTAGE

An automated incident response and remediation workflow reduces phishing incident response time by up to 95%.

Integrate out-of-the-box with Microsoft Office 365 to automatically remove all phishing emails from user inboxes.

URL, attachment, and sender forensics enables fast and accurate investigation.

Impact analysis showcases the number of employees susceptible to a potential breach.

Accelerate Phishing Response Time

Agari Incident Response is the only turnkey phishing incident response solution that seamlessly integrates with Microsoft Office 365 to automatically remove all phishing emails from user inboxes. The solution delivers detailed impact analysis, enabling security teams to ignore false positives and slashing phishing incident response times.

By streamlining response times and automatically removing malicious emails from inboxes, Agari Incident Response contains breaches in minutes instead of months.

Agari Incident Response Automated Phishing Playbook

Agari Incident Response provides an end-to-end automated phishing playbook that integrates with Microsoft Office 365 to handle employee phishing reports, triage them, remove false positives, perform forensic analysis, and then automate the remediation process:

REPORTING

Employees report phishing incidents through a phish button, abuse email address, or helpdesk support ticket.

TRIAGE

A SOC analyst quickly reviews the sender's identity, their trust level, attributes of the email, and whether it contains malicious attachments, URLs, or content.

FORENSICS

The SOC analyst reviews forensic information about the email to complete an investigation.

REMEDIATION

The SOC analyst determines and applies the necessary remediation action, such as removing emails from inboxes or resetting account passwords..

The Company We Keep

Top 3 Social Networks | 6 of the Top 10 Banks | Top Cloud Providers

Microsoft HSBC aetna facebook citi CHASE Google

Learn More: www.agari.com/products

[1] Verizon Data Breach Digest 2017