AREA 1

Microsoft Partner

Microsoft

Partner of the Year

Google Cloud

AUTONOMOUS PHISH SOC

Close the Phish Gap. Improve SOC Agility and Efficiency.

PROBLEM

- Increased end user reports of suspicious emails
- SOC inefficiencies due to manual correlations (6-8 hours per incident) and retractions
- Phish missed by SEGs and other traditional defenses

SOLUTION

- **Close The Phish Gap:** Identify and remove the phish that bypass your email providers and SEGs
- **Enhance Signals & Reduce Noise:** Analyze end user reports rapidly, and focus on true signals to prioritize incidents that need SOC oversight
- **Improve Response Times:** Reduce time and effort spent in phish investigations by at least 90 percent

SOLUTION OVERVIEW

Missed phish and inefficiency in traditional Security Operations Center (SOC) tools make cybersecurity investigations costly and time-consuming. Area 1 Security's Autonomous Phish SOC closes the phish gap by catching and removing the phish that other security products miss, saving time and money.

SOC teams today are inundated with missed phish bypassing existing cloud providers and secure email gateways (SEGs) to land in inboxes, and end user reports that need continuous investigations and follow-up. For security teams, Area 1's Autonomous Phish SOC's enhanced signals, full context and built-in remediation allow for better and faster incident resolution.

Features like automated triage and detection search APIs help streamline routine processes and reduce manual efforts. Flexible response options including native remediation with Message Retraction and integrations with orchestration tools of the customer's choice lets analysts focus — and take immediate action on — real threats.

Purpose-built to improve security response times, remediate and eliminate critical phishing incidents, the Autonomous Phish SOC's end-to-end detection-to-response capabilities decrease incident triage time by up to 90% and significantly improves the security posture of organizations struggling with missed phish.

SOC teams face several major challenges which result in prolonged investigations and delayed incident response (IR):

- Detection failures
- High volumes of user-reported phish
- The lack of good forensics
- Cumbersome remediation processes that involves multiple teams and tools

AREA 1

These challenges generate inefficiencies in SOC processes, costing valuable time and resources.

Office 365, Gmail and legacy email gateways also miss a high volume of phishing emails. End user reports focus not only on the misses but non-misses as well, which become a greater burden for security teams to analyze and sift through.

The noise levels are high. For abuse inbox and incident triage, the lack of context and forensics results in extended investigations. Triage and manual correlations cost an average of six to eight hours per incident.

Even when incidents have been fully investigated, remediation and removal of malicious messages can be a cumbersome and time consuming process. This usually results in tickets bounced between SOC, Messaging and IT teams or the maintenance of custom Microsoft scripts to remove emails from inboxes.

CURRENT SOC CHALLENGES

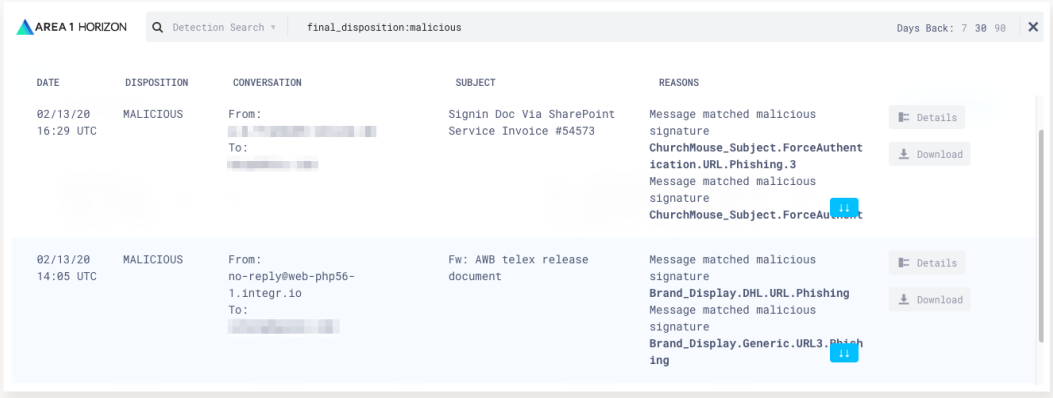
01	02	03	04
DETECTION FAILURES	**HIGH VOLUME OF USER-REPORTED PHISH**	**LACK OF GOOD FORENSICS**	**MANUAL & TIME-CONSUMING INVESTIGATIONS**

Area 1 Security's Autonomous Phish SOC solves the key challenges of detection, response and manual inefficiency involved with triaging and dealing with missed phish.

The Autonomous Phish SOC detects 99.997% of all phish messages. With a closed phish gap and better protection for end-users, employees no longer flood abuse inboxes with internal reports and false positives.

Designed to enable quick investigations, the Autonomous Phish SOC provides all necessary information in an easy-to-access manner for SOC teams. Detections come packaged with multi-level forensics for message headers, message bodies, and any URLs and attachments.

Additional enrichment and context such as associated actor, campaign, and indicators of compromise (IOCs) are all readily available so security staff aren't spending time on manual correlations.

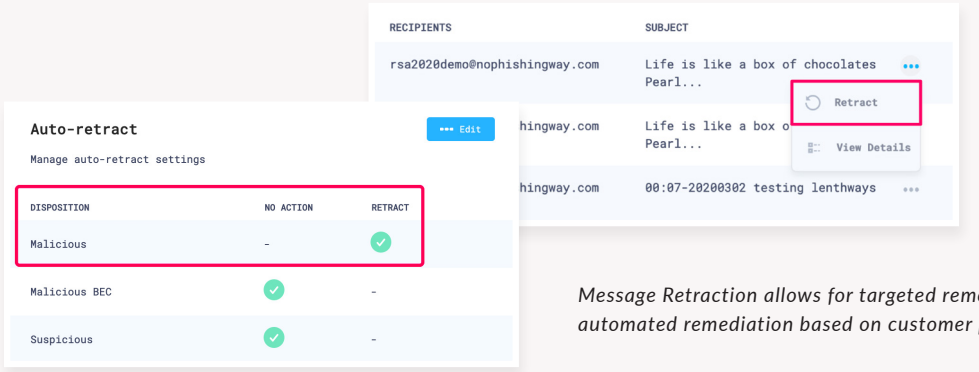


Associated forensics are displayed with detections for easy triage.

Area 1's cloud-native infrastructure makes deployment quick, simple, and flexible. A variety of email ingestion options are available including offline or BCC mode, journaling, or via API. Cloud-powered architecture also accommodates rapid-scale indexing and retrieval so results are immediate. Intuitive interfaces and unfaceted, Google-like search capabilities also make information easy-to-access.

The Autonomous Phish SOC's enhanced signals and built-in response options ultimately result in significantly better security & improved incident response times. Our customers have been able to decrease triage time by as much as 90%. With built-in automated triage, analysts receive simple message dispositions for follow-up actions. This enables analysts to easily prioritize the incidents that need actual human oversight.

A host of features have also been developed to automate routine SOC tasks. For example, detection search APIs with tokenized search parameters allow for repeatable, automated pulls of specific phish detections. Even remediation can be automated. Our Message Retraction feature can be combined with an auto-retraction policy to automate the removal of malicious messages from all inboxes. Alternatively, targeted remediation allows analysts to review detections and remove malicious messages with a click of a button. Both Message Retraction options allow SOC teams to neutralize threats even in cases when Area 1 is deployed in BCC or journaling mode.



Message Retraction allows for targeted remediation or automated remediation based on customer policies.

AREA 1

Streamlined integration with security information and event management (SIEM) systems and API hooks into SOARs further allow for fully customizable response playbooks.

1 **REMOVE THE PHISH GAP**

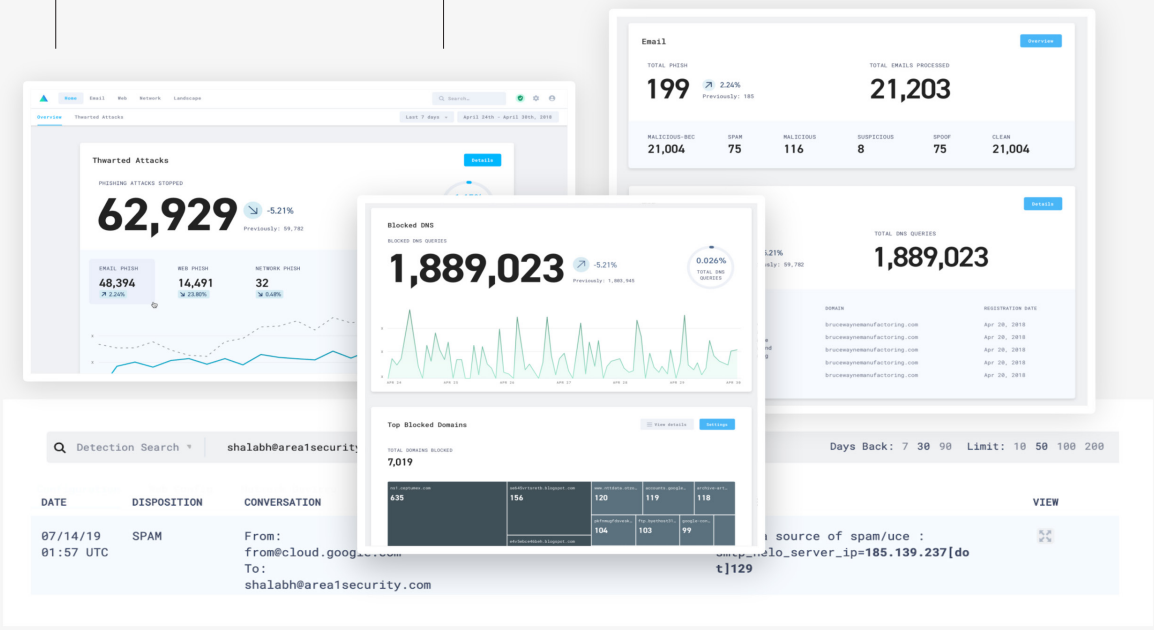
Address missed phish that bypass existing gateways

2 **ENHANCE SIGNAL / IGNORE NOISE**

Focus on true signals / tier 1 incidents that need SOC oversight

3 **IMPROVE RESPONSE TIME**

Reduce time and effort spent in phish investigations by 90%



AREA 1

1

QUICK AND EASY DEPLOYMENTS:

Fully scalable cloud-native architecture with no tuning required. Offline / BCC, journaling, and APIs for transparent visibility and no impact to current operations.

2

AUTOMATED DETECTIONS AND TRIAGE:

First and second level triage with message dispositions for follow-up action. Automated detection searches via API.

3

RAPID SCALE INDEXING AND RETRIEVAL:

Immediate results and flexible search parameters with faceted or unfaceted natural language search.

4

MULTI-LEVEL FORENSICS:

Deep analytics of triaged incidents complete with details on message headers, message bodies, URLs, and attachments.

5

ENRICHMENT AND CONTEXT:

Detailed actor, campaign, and IOC analysis

6

ORCHESTRATION AND REMEDIATION:

Built-in remediation with Message Retraction and integration with SIEMs /SOARs for customized playbooks and responses

Area 1's Autonomous Phish SOC closes the phish gap, enables rapid resolutions of end user reports, and automates triaging and remediation processes so your security talent can focus on more interesting and productive work.

For a free demo, visit www.area1security.com/try-area1.

About Area 1 Security

Area 1 Security offers the only pay-for-performance solution in the cybersecurity industry - and the only technology that comprehensively blocks phishing attacks before they damage your business. Phishing is the root cause of 95 percent of security breaches.

Area 1 Security works with some of the most sophisticated organizations in the world, including Fortune 500 banks, insurance companies, and healthcare providers to preempt and stop targeted phishing attacks at the outset, improve their cybersecurity posture and change outcomes.

Learn more at www.area1security.com, join the conversation at @area1security or subscribe to the Phish of the Week for the latest industry news and insights on how to deal with phishing.