CLOUDFLARE
AREA 1 SECURITY

Phish Submission Triage

Phish Submission Guide

Area 1 Horizon Overview

Phishing is the root cause of 95% of security breaches that lead to financial loss and brand damage. Area 1 Horizon is a cloud based service that stops phishing attacks, the #1 cybersecurity threat, across all traffic vectors - email, web and network.

With globally distributed sensors & comprehensive attack analytics, Area 1 Horizon proactively identifies phishing campaigns, attacker infrastructure, and attack delivery mechanisms during the earliest stages of a phishing attack cycle. Using flexible enforcement platforms, Area 1 Horizon allows customers to take preemptive action against these targeted phishing attacks across all vectors - email, web and network; either at the edge or in the cloud.

Phish Submission Triage

Phish submission triage is a process where customers can submit missed phish samples to Area 1, the samples will be processed to take necessary action.

1. How do I find my phish submission addresses?

The addresses are listed here:
https://horizon.area1security.com/support/service-addresses

2. Two different ways to submit a Phish

Users submission:

To be used with phish submission buttons. Submitted directly by the end users.
Please refer to the below article to configure Phish Submission Button on Outlook:
https://area1security.zendesk.com/hc/en-us/articles/1500006024362-Report-Phish-from-Outlook-client-to-Area-1

Team submissions:

To be used when IT administrators or Security teams submits to Area 1. Phish samples submitted to this address will be considered as submissions from the customer's email security team and hence increases the chances of similar samples being detected as malicious in the future. Please submit original phish samples as an attachment in .eml format to the ***team submission*** address.

Please find more details here:
https://area1security.zendesk.com/hc/en-us/articles/4411817834643-False-Positive-or-False-Negative-Submission-Addresses-

3. Why was Phish missed?

We make use of several techniques to make a detection such as preemptively crawling the web to identify campaigns, machine learning, custom signatures, intel feed from other sources etc.

In order for us to identify why this was missed, we need to run the original samples through our module (and identify why some of our modules didn't score the sample high enough to elevate it to malicious).

4. What happens after phish submission?

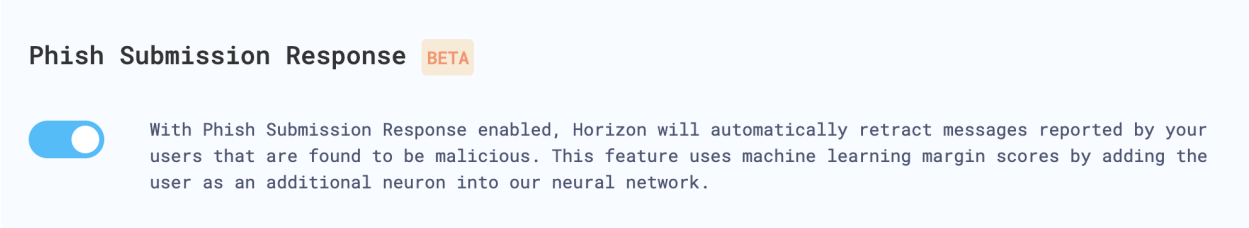
Machine learning:

After submitting the phish sample to a special email address provisioned for you, the sample will be added directly into our machine learning queue. As soon as you send something it will be automatically processed by our ML module for learning. Some samples will be directly converted to malicious upon going through machine learning and rest will be further processed by our ML module.

Phish Submission Response

With Phish Submission Response enabled, Horizon will automatically retract messages reported by your users that are found to be malicious. This feature uses machine learning margin scores by adding the user as an additional neuron into our neural network.

In order to enable PSR, navigate to the following location on the Area 1 portal and toggle the PSR switch:
https://horizon.area1security.com/settings/email/retract-settings/automatic-retract



Note: PSR works only for the phish samples submitted to user submission addresses.

Please refer to the following articles to configure retraction:
1> O365 message retraction configuration:
https://area1security.zendesk.com/hc/en-us/articles/360050127393-Microsoft-O365-Message-Retraction
2> Gmail message retraction configuration:

https://area1security.zendesk.com/hc/en-us/articles/360059152954-GSuite-Gmail-Message-Retraction-Guide

5. How to obtain feedback on phish submission?

Detection search:

Using the keyword 'phish_submission' or 'user_malicious_submission' or 'team_malicious_submission' you can look for the submitted phish samples on Area 1 portal detection search. On the 'Alert Reason' column you will see the feedback. If the ML module learns and detects it as phish then on the 'Alert Reason' column you will see the details. If not it will just show up as 'phish submission'.

Contacting Support:

If there is a phishing email that is repeatedly sent to users despite being submitted to Area 1 for processing earlier, then please contact support with details of phish submission (alert ID or message ID of the sample).