Incident Responder

MANAGE REPORTED EMAILS THROUGH AUTOMATED ANALYSIS AND INVESTIGATION

Summary

The Challenge

Responding swiftly to email attacks is significant, as each passing minute escalates the threat. On average, it takes **9 hours** to detect and remove a malicious email, significantly amplifying the risk.

Our Solution

Our automated phishing incident response tool allows businesses to identify and respond to email attacks in **minutes**

Agenda

1

Default Bahvaiour of IR

How the Incdient Responder works when using the default behaviour

2

Technical Setup Requirements

The integrations needed for Incdient Responder to work successfully

3

Optional Customisations

Changing the default behaviour to align closely with you business objectives

Default Behaviour of Incident Responder

Step 1: Analysis

STEP 1

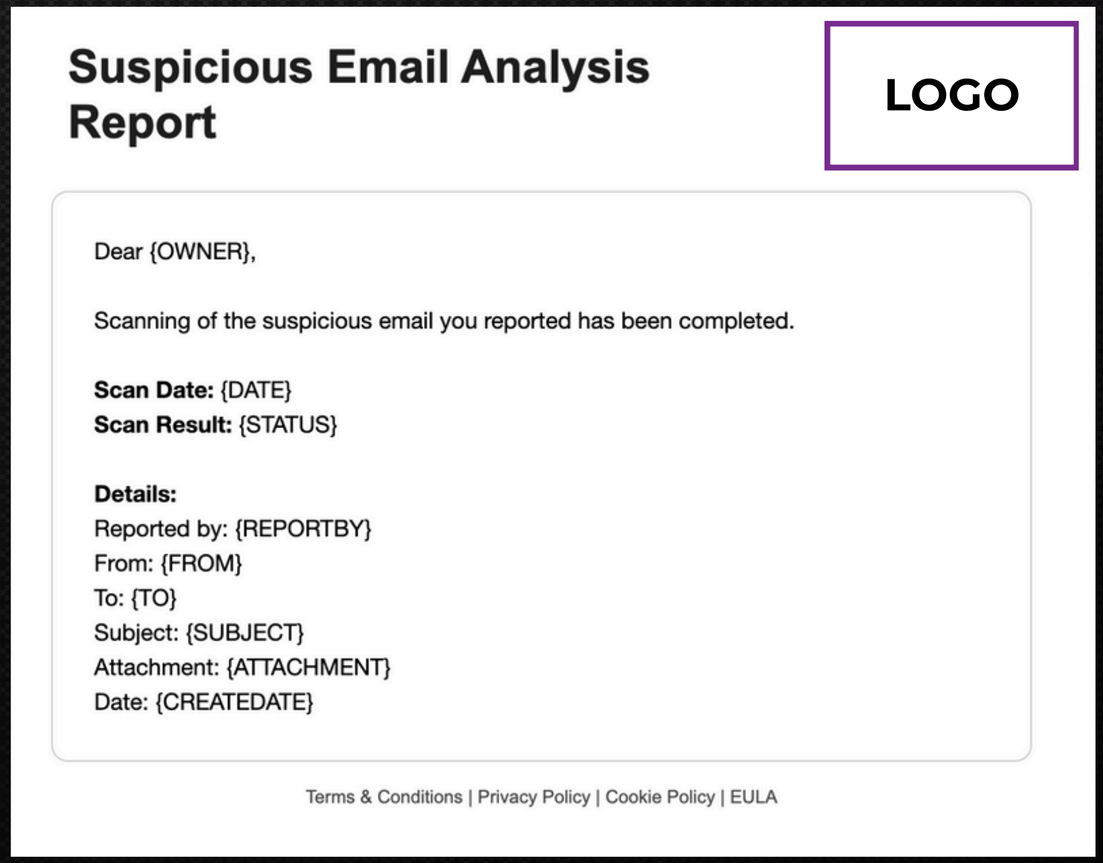
An employee reports a suspicious email using the *Customisable Reporter Button* or *Native Microsoft Report button*

STEP 2

Incident Responder analysis the reported email for malicious content in seconds using 5+ integrations simulatenously

STEP 3

Incident Responder automatically shares the analysis result with the employee via email (template here ->)



Suspicious Email Analysis Report

LOGO

Dear {OWNER},

Scanning of the suspicious email you reported has been completed.

Scan Date: {DATE}
Scan Result: {STATUS}

Details:
Reported by: {REPORTBY}
From: {FROM}
To: {TO}
Subject: {SUBJECT}
Attachment: {ATTACHMENT}
Date: {CREATEDATE}

Terms & Conditions | Privacy Policy | Cookie Policy | EULA

Default Behaviour of Incident Responder

Step 2: Investigation

STEP 1

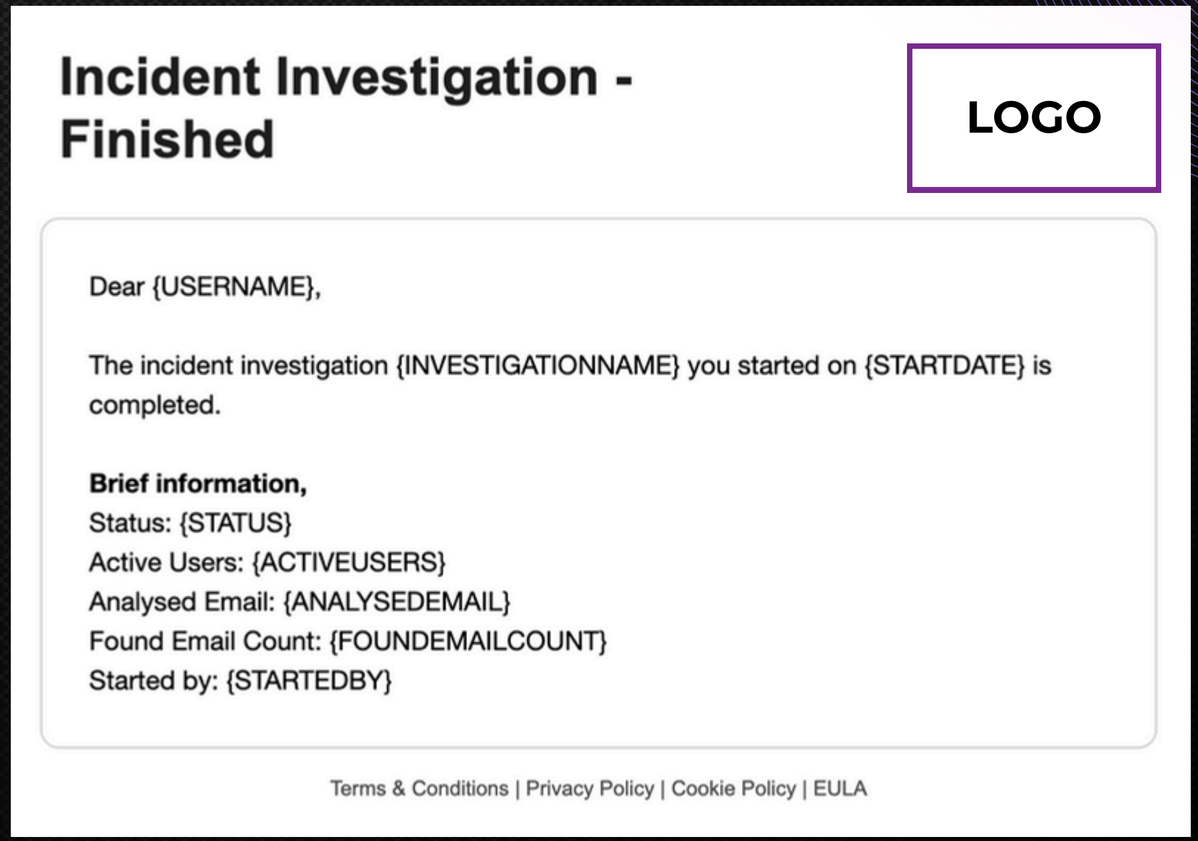
When analysis result is “Malicious”, Incident Responder starts an automatic investigation to find all instances of the malicious content

STEP 2

Once investigation is complete, System Admins recceive Investigation Reporrt

STEP 3

System Admins can then log into Keepnet and delete all instances of malicious emails in a few clicks



Technical Setup for Incident Responder

Step 1: ANALYSIS
Add several integrations to the platform to analyse emails for malicious content. For example Fortinet Sandbox

The expectation is that customers add their own accounts for each analysis tool into the platform

No permissions required

How to add a new integration

Step 2: INVESTIGATION
Set up a mail configuration so Incident Responder can find all instances where the malicious content exists in your entire email estate and delete all instances.

Permissions Required:

- Directory.Read.All
- Mail.ReadWrite
- MailboxSettings.ReadWrite
- User.Read.All (under User)

How to set up mail configuration

Custom Default Behaviour Optional

Auto-Delete Malicious Emails

You can create a playbook which **automatically deletes** all instances of malicious content

Custom Notifications

Customers can customise the entire notification templates employees receive

Notify a Specific Inbox

Customers can change the default behaviour to notify a specific inbox of all analysis reports

SOAR Integrations

Native integration with Palo Alto XSOAR, IBM Resilience, Splunk and other SOAR solutions,