CLOUDGUARD SAAS THREAT EXTRACTION

December 2018

Brian Heffner
bheffner@checkpoint.com

Overview

- The purpose of this whitepaper is to explain a confusing Threat Extraction "scan details" action within CloudGuard SaaS. I will be focusing on something called **"should replace."** We will be focused on the Threat Protection portion of the portal and not the Identity Protection portion. In addition, we will NOT be reviewing DLP.

  - CLOUDGUARD SAAS - SAAS SECURITY IS ONE CLICK AWAY
    - To protect from SaaS threats, Check Point offers CloudGuard SaaS – a new cloud service that prevents attacks on enterprise SaaS applications, within minutes' deployment.
    - Prevent malware and zero-day threats from getting into SaaS apps
    - Blocks cybercriminals from taking over employee SaaS accounts with ID-Guard technology
    - Keeps data protected by blocking sensitive data sharing and forcing its encryption
    - Provides full security coverage with synced policies and unified management across gateways, endpoints, and cloud

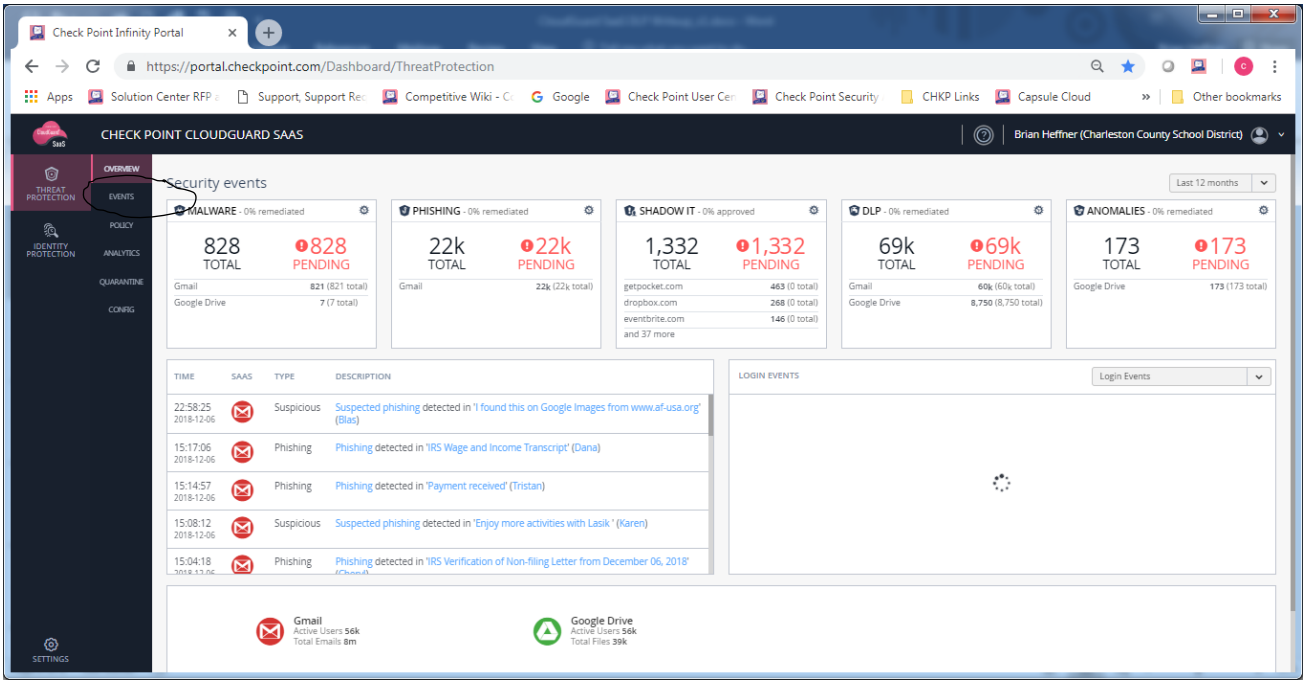
Assumptions & Requirements

This guide makes the following assumptions:

- Your Check Point Cloud portal at https://portal.checkpoint.com is already provisioned and you have your login name and password.
- You have already configured the API connection for your SaaS application.

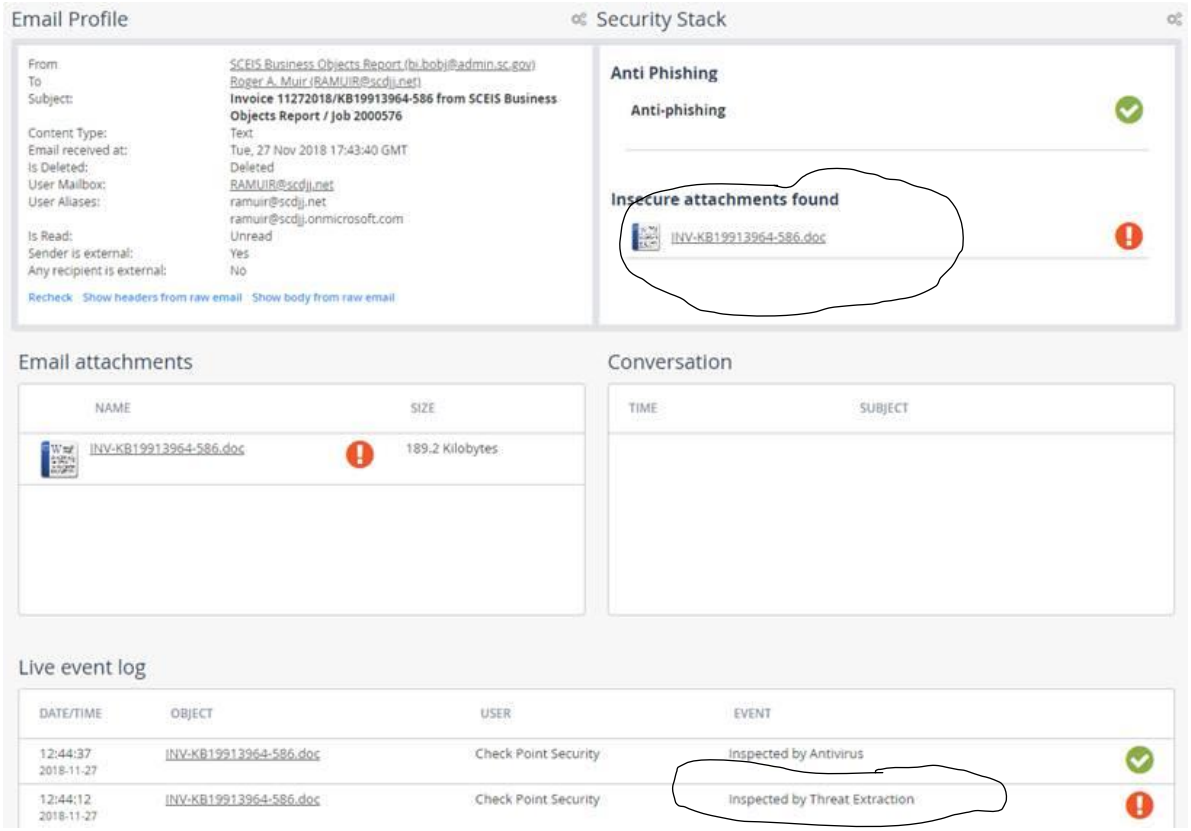
ENVIRONMENT PROBLEM

CloudGuard SaaS portal already setup against Microsoft or Google email.
After you login to https://portal.checkpoint.com, you will see the overview page.
Here is a sample:

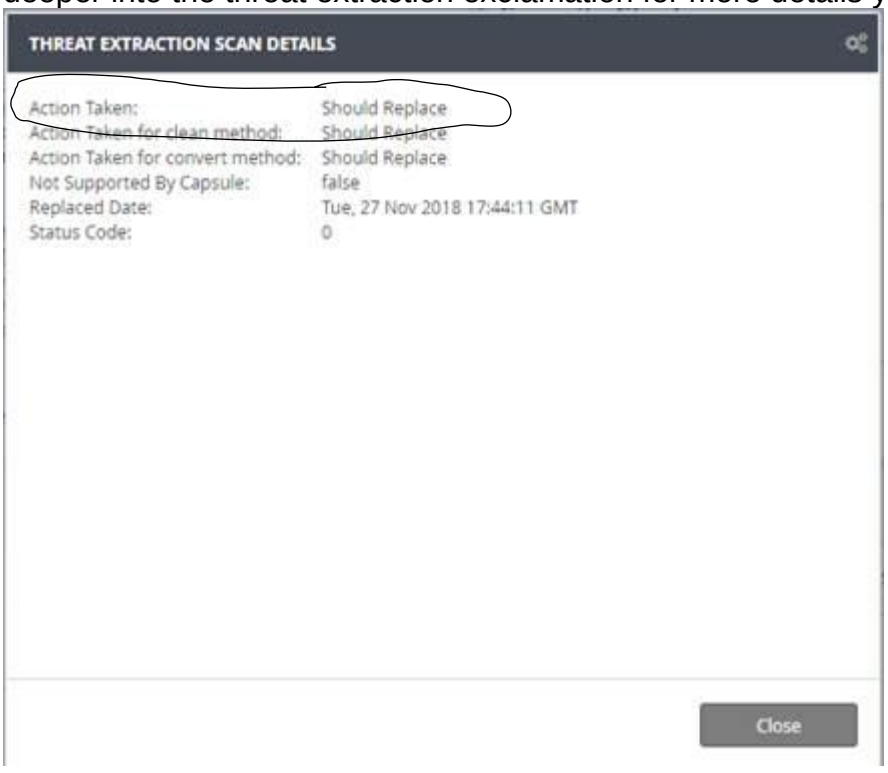


Next, you would choose EVENTS from the menu on the left side of the overview page.

Here is a sample screen of an event you would normally see:



You will see from screen shot above, a typical alert that anti-phishing says the email is fine. However, the exclamation point for the attachment will stand out to you. When you dive deeper into the threat extraction exclamation for more details you will get this screen:

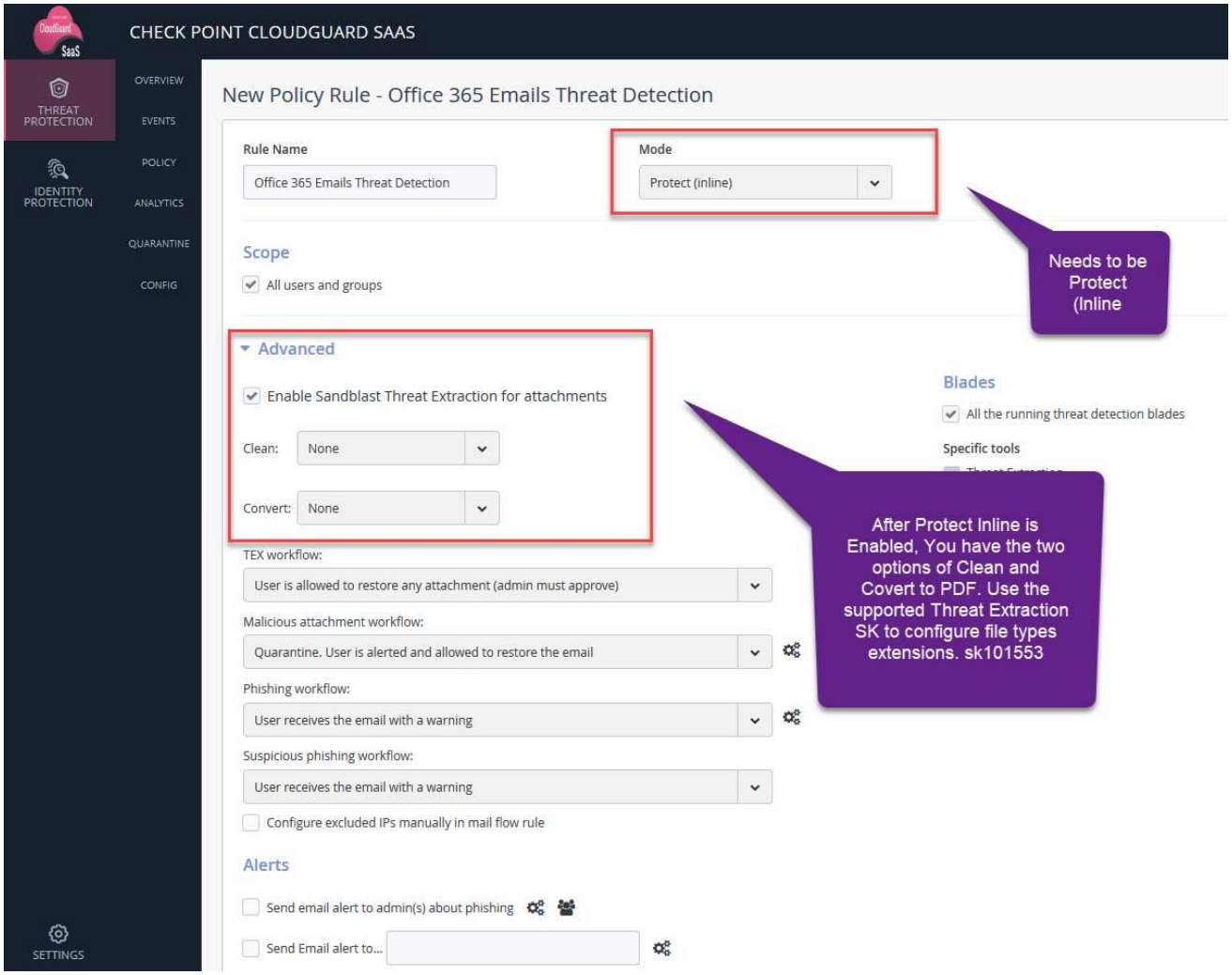


Here is the problem. What exactly is an action taken of **"should replace?"** If the action was really "taken" then there is no "should" because it would be done. However, my customer wanted an explanation and so did I. I was unable to find any details about this anywhere. Therefore, it was time for R&D help.

RESOLUTION

When you see this confusing status it means that **"IF"** you had threat extraction enabled then threat extraction would have replaced the attachment with a clean PDF. So in my situation, since TE was not enabled, then the malicious file was not converted. Therefore, leaving the mailbox vulnerable. To protect yourself from this confusing situation with your customer and to help them be better protected, TE must be enabled.

The steps to enable TE are very easy. You simply create a new threat protection rule as below with the highlighted mode and advanced settings.



Additional Resources

1. Check Point CloudGuard SaaS Getting Started Guide
2. Check Point CloudGuard SaaS Identity Protection Guide
3. Check Point CloudGuard SaaS Manual Configuration with Office 365
4. Check Point CloudGuard SaaS Threat Protection Admin Guide
5. Check Point Infinity Portal Admin Guide

All documents above available from this link:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doShowproductpage&product=495

